THESE de DOCTORAT DE L'UNIVERSITE DE LYON

Opérée au sein de

INSA Lyon

Ecole Doctorale EDA 512

Informatique et Mathématique de Lyon

Spécialité/ discipline de doctorat : Informatique

Soutenue publiquement le 29/07/2020, par :

Abderrahman BEN KHALIFA

Medium Access Control Layer for Dedicated IoT Networks

Devant le jury composé de :

Antoine GALLAIS	Professeur	Université Polytechnique Hauts de France	Rapporteur
Congduc PHAM	Professeur	Université de Pau et des Pays de l'Adour	Rapporteur
Nancy EL RACHKIDY	Maître de Conférences	Université Clermont Auvergne	Examinateur
Mickael MAMAN	Ingénieur de Recherche	CEA LETI	Examinateur
Hervé RIVANO	Professeur	INSA Lyon	Directeur de thèse
Razvan STANICA	Maître de Conférences	INSA Lyon	Co-directeur de thèse

Abstract

Dedicated networks for the Internet of Things appeared with the promise of connecting thousands of nodes, or even more, to a single base station in a star topology. This new logic represents a fundamental change in the way of thinking about networks, after decades during which research work mainly focused on multi-hop networks.

Internet of Things networks are characterized by long transmission range, wide geographic coverage, low energy consumption and low set-up costs. This made it necessary to adapt the protocols at different architectural layers in order to meet the needs of these networks.

Several players compete in the Internet of Things market, each trying to establish the most efficient solution. These players are mostly focused on modifying the physical layer, on the hardware part or through proposing new modulations. However, with regard to the channel access control solution (known as the MAC protocol), all the solutions proposed by these players are based on classic approaches such as Aloha and CSMA.

The objective of this thesis is to propose a dynamic MAC solution for networks dedicated to the Internet of Things. The proposed solution has the ability to adapt to network conditions. This solution is based on a machine learning algorithm that learns from network history in order to establish the relationship between network conditions, MAC layer parameters and network performance in terms of reliability and energy consumption. The solution also has the originality of making possible the coexistence of nodes using different MAC configurations within the same network. The results of simulations have shown that a MAC solution based on machine learning could take advantage of the good properties of different conventional MAC protocols. The results also show that a cognitive MAC solution always offers the best compromise between reliability and energy consumption, while taking into account the fairness between the nodes of the network. The cognitive MAC solution tested for high density networks has proven better scalability compared to conventional MAC protocols, which is another important advantage of our solution.

Résumé

Les réseaux dédiés pour l'Internet des Objets sont apparus avec la promesse de connecter des milliers de nœuds, voire plus, à une seule station de base dans une topologie en étoile. Cette nouvelle logique représente un changement fondamental dans la façon de penser les réseaux, après des décennies pendant lesquelles les travaux de recherche se sont focalisés sur les réseaux multi-sauts.

Les réseaux pour l'Internet des Objets se caractérisent par la longue portée des transmissions, la vaste couverture géographique, une faible consommation d'énergie et un bas coût de mise en place. Cela a rendu nécessaire des adaptations à tous les niveaux protocolaires afin de satisfaire les besoins de ces réseaux.

Plusieurs acteurs sont en concurrence sur le marché de l'Internet des Objets, essayant chacun d'établir la solution la plus efficiente. Ces acteurs se sont concentrés sur la modification de la couche physique, soit au niveau de la partie matérielle, soit par la proposition de nouvelles techniques de modulation. Toutefois, en ce qui concerne la solution de contrôle d'accès au canal (connue sous le nom de couche MAC), toutes les solutions proposées par ces acteurs se fondent sur des approches classiques, tel que Aloha et CSMA.

L'objectif de cette thèse est de proposer une solution MAC dynamique pour les réseaux dédiés à l'Internet des Objets. La solution proposée a la capacité de s'adapter aux conditions du réseau. Cette solution est basée sur un algorithme d'apprentissage automatique, qui apprend de l'historique du réseau afin d'établir la relation entre les conditions du réseau, les paramètres de la couche MAC et les performances du réseau en termes de fiabilité et de consommation d'énergie. La solution possède également l'originalité de faire coexister des nœuds utilisant de différentes configurations MAC au sein du même réseau. Les résultats de simulations ont montré qu'une solution MAC basée sur l'apprentissage automatique pourrait tirer profit des avantages des différents protocoles MAC classiques. Les résultats montrent aussi qu'une solution MAC cognitive offre toujours le meilleur compromis entre fiabilité et consommation d'énergie, tout en prenant en compte l'équité entre les nœuds du réseau. La solution MAC cognitive testée pour des réseaux à haute densité a prouvé des bonnes propriétés de passage à l'échelle par rapport aux protocoles MACs classiques, ce qui constitue un autre atout important de notre solution.

Remerciements

Il me sera très difficile de remercier en une seule page toutes les personnes qui ont contribué directement et indirectement à la réalisation de cette thèse.

Avant tout, je voudrais exprimer ma sincère gratitude à mon encadrant Dr. Razvan STANICA pour m'avoir donné l'opportunité de faire un doctorat et de découvrir le monde de la recherche. Sa patience, sa motivation, son soutien et sa confiance m'ont aidé tout au long de la recherche et de la réalisation de cette thèse. Il était toujours là pour écouter, discuter de mes idées et me poser de bonnes questions pour enrichir mon travail. J'ai apprécié énormément ses conseils et ses encouragements : ce fut une grande chance d'apprendre de lui.

Ma gratitude va également au professeur Hervé RIVANO, mon directeur de thèse, pour le soutien tout au long de mon doctorat, pour sa motivation, son enthousiasme et ses grandes connaissances. Je le remercie énormément de m'avoir accueilli et de m'avoir initié au monde de la recherche.

Je tiens à remercier les membres du jury d'avoir accepté de réviser ma thèse, d'avoir consacré leur temps à la lire et de m'avoir fait de précieux commentaires.

J'en profite pour remercier mes chers collègues du laboratoire CITI d'avoir partagé leurs travaux. Je remercie également les personnels administratifs du CITI et plus particulièrement les assistantes de l'équipe Agora. Je dois remercier tout spécialement tous mes amis de l'équipe Agora pour les discussions stimulantes et les moments inoubliables que nous avons eu au cours des trois dernières années.

Enfin, Mes remerciements ne seraient pas complets sans remercier mes parents qui m'ont entouré, tout au long de mes études, de leur patience et de leur compréhension, ainsi que mes frères, mes sœurs et ma famille. Je tiens à exprimer ma gratitude particulière à ma femme bien-aimée, sans elle, cette thèse n'aurait jamais vu le jour, pour son soutien moral, sa motivation, ses encouragements, ses précieux conseils et plus encore pour l'amour qu'elle m'a montré toutes ces années.

Contents

List of Figures

List of Tables

List of Abbreviations

IoT	Internet of Things
LPWAN	Low Power Wide Area Network
NB-IoT	Narrow Band IoT
3GPP	3rd Generation Partnership Project
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
CDMA	Code Division Multiple Access
SMACS	Self-organizing Medium Access Control for Sensor Networks
RTS	Request-To-Send
CTS	Clear-To-Send

1. Introduction

After almost two decades of research on multi-hop short range wireless sensor networks, we are witnessing today a paradigm shift, where small, energy constrained *things* are connected to the rest of the world through one-hop, cellular-like dedicated networks, also described as low-power wide area networks (LPWAN) [13]. Multiple technologies are competing in this dedicated Internet of Things (IoT) market, either proposed by new players (*e.g.* Sigfox [14], LoRa [15]), or backed up by well-established standardization bodies (*e.g.* NB-IoT from the 3GPP consortium [16], or IEEE 802.11ah from the WiFi Alliance[17]).

Practically, dedicated IoT networks are characterized by a cellular architecture, with a central base station or gateway, collecting data from a number of objects in its coverage. Another common characteristic of all these technologies is that they follow one of two classical channel access schemes: Aloha or Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The only modification brought to these classical approaches is that, in some technologies, Aloha is modified in order to not transmit acknowledgment (ACK) messages, generally because a down-link is not always available in these networks, or it is very limited.

Basically, three main MAC layer solutions are currently competing in the IoT world. First of all, the technologies coming from the 3GPP world, whether LTE-M or NB-IoT [18], are using classical Aloha solutions. More precisely, these technologies use a slotted-Aloha approach [19], where nodes can only access the medium on specific time-frequency blocks of the LTE random access channel.

A second class of IoT technologies, commonly designated as LPWANs, is also based on an Aloha MAC protocol. Indeed, Aloha is a very simple strategy, where the MAC layer directly transmits any message produced by the application layer. Easy to implement and without any strong synchronization requirements, Aloha was the obvious choice for new technologies, such as Sigfox [14] and LoRa [15]. However, these technologies also needed to cope with the well-known poor scalability of Aloha; this was done by over-provisioning, the temporal Aloha space being expanded in the frequency domain (e.g. in Sigfox) or in the code domain (e.g. in LoRa). Moreover, these technologies are generally asymmetrical, meaning that the downlink is very limited. This has a direct consequence on the MAC layer, as the gateway does not acknowledge the reception of data messages from the nodes.

Finally, the most successful wireless technology nowadays, WiFi, is also looking for a place in the IoT world, through a recent amendment known as WiFi HaLow, and standardized as IEEE 802.11ah [17]. As all the technologies from the IEEE 802.11 family, WiFi HaLow is based on a CSMA/CA MAC layer. The main difference with respect to the classical Distributed Contention Function (DCF) used in IEEE 802.11 is that the existing stations are divided into groups, and the contention only happens between stations from the same group. The gateway defines the different time intervals for each contending group.

The medium access control in IoT networks is therefore mainly based on static approaches. In the Aloha-based MAC protocols, a node randomly selects a resource from the resource space, with no coordination with other nodes. The Aloha family of protocols is commonly known for its poor performance, and its usage in IoT networks is only made possible by a combination of low penetration ratio of IoT devices, which is foreseen to highly increase in the near future, and a very large resource space, which is already close to the maximum limit. Meanwhile, the connection of personal objects in a home (in the order of tens of objects) to a local access point uses a carrier sense multiple access approach (generally CSMA/CA) at the MAC layer, a solution which also presents known scalability problems.

The starting point of this thesis is the belief that one of the best enhancements to bring to the MAC layer is to add intelligence to it. This could be done with a machine learning approach that capitalizes the past experience of the network in order to tune the MAC configuration in a way that suits the network situation (device distribution in the cell, traffic intensity, channel quality, etc.). Then, the

cognitive MAC solution would smartly adapt the MAC layer configuration to the network dynamics, and will be able to take benefit of both Aloha and CSMA, or other future MAC protocols.

Throughout this work, we present our proposition of a cognitive MAC protocol for dedicated IoT networks. The cognitive MAC solution is based on a machine learning algorithm, that exploits the network history to propose a suitable MAC configuration distribution in order to get the best performance. The MAC configuration is more general than a MAC protocol and it represents nothing else than a specific setting of the MAC layer parameters. Thus, changing the value of one of the MAC layer parameter changes the MAC configuration.

The coexistence of different MAC configurations within the same cell was already studied in the literature [62] without showing any enhancement promises. In our solution, we show that a machine learning algorithm is capable of taking benefit of a hybrid network configuration, where devices use different MAC approaches.

To accomplish our targeted MAC strategy, we followed a certain methodology, and every key step of this methodology is presented in a chapter in the remainder of this document.

In Chapter 3, we first define the performance evaluation metrics that are suitable for the context of dedicated IoT networks. More precisely, the transmission reliability and the energy consumption are the most important metrics for the majority of the IoT networks applications. We use the packet success probability as an indicator of the transmission reliability, while for the energy consumption we use the time that a node spends in an active ON state in order to offer a technology agnostic energy measurement. Then, we use simulations in order to evaluate the performance of networks using an Aloha-based and a CSMA-based MAC solution, while variating a set of MAC parameters and changing the network condition in terms of density of the nodes and generated traffic. The main conclusions of this chapter are that there is no universal MAC configuration and the best MAC solution depends on several factors. Moreover, we notice that the acknowledgment messages decrease the IoT network performance and the number of frame retransmissions is a MAC layer parameter that impacts significantly the IoT network performance.

In Chapter 4, we study the Aloha MAC protocol performance with simulation and analytical modeling. The studied Aloha protocol does not use acknowledgment messages, and we denote it as Aloha No Ack. In the chapter, we focus on the MAC frame retransmission number. We study through an original analytical model how the network performance changes with the variation of this parameter, under different network conditions. Afterward, we exploit the analytical model to get the optimal value in terms of frame retransmissions for each network condition. Interestingly, the optimal value in many cases is not the highest value, which means retransmitting more does not imply better reliability. At the end of the chapter, we compare Aloha No Ack with an optimal frame retransmission number and the Aloha flavor used by SigFox. The results show the gap between current state of the art solutions and an optimal MAC configuration, under many traffic conditions, in terms of reliability and energy consumption.

In Chapter 5, we study a CSMA based MAC solution for IoT networks, where the acknowledgement messages are not used. This solution is denoted as CSMA No Ack. Many contributions tended to propose CSMA based MAC solution for IoT networks. However, all of them ignored a major parameter of this protocol, which is the Clear Channel Assessment (CCA) threshold, which directly reflects the receiver sensitivity of the devices. We consider that the usage of the CSMA protocol in the case of IoT networks is constrained by the poor sensitivity of low cost IoT devices. Therefore, we believe that a realistic study of CSMA based MAC implementation for LPWAN should take into account the CCA threshold parameter. Hence, we start the chapter by studying the impact of this parameter; as explained, the CCA threshold represents the receiver sensitivity and reflects the capacity of a node to sense other simultaneous transmissions, and hence avoid collisions. We show, with simulation results, how this parameter influences the performance of the network. We note that the CCA threshold is a hardware related parameter and that, in a real IoT network, it could not be an easily tunable MAC layer parameter. Therefore, we present in this chapter a CSMA No Ack implementation with realistic receiver sensitivity. Afterward, following the same logic as in the previous chapter, we study the impact of the frame retransmission number on the CSMA No Ack

network. At the end of the chapter, we compare between CSMA No Ack and Aloha No Ack, while both are configured to use an optimal frame retransmission number.

In Chapter 6, we present the implementation of a machine learning based MAC solution for dedicated IoT networks. We started by training different machine learning solutions with the data generated by simulations, and after an exhaustive test phase we selected the algorithm that achieved the highest accuracy rate, which is based on Convolutional Neural Networks (CNN). The input data is constituted of the MAC layer configuration of the device (set of key parameters), the distance separating the device from the gateway and the network density. While for the output, we have two informations reflecting the network performance metrics: the packet success probability and the node activity time. Once the CNN solution is implemented, we started by validating the predicted outputs against simulation results on new scenarios, not used in the training process. Then, we used the CNN approach to predict the most suitable MAC configuration distribution per node for different network situations. With simulation results, we proved the superiority of our proposed cognitive solution, denoted as ML MAC, with respect to classical MAC protocols. For a high-dense network, our solution presents 30% better reliability, while offering an energy saving behavior, which reflects the good scalability of our technique. For a medium-dense network, the improvement of reliability reaches 50%, which represents a promising result of machine learning based MAC efficiency. For both network densities, the ML MAC showed a better fairness in the results. Meanwhile, for some scenarios, classical MAC approaches showed a poor fairness: the Aloha based solutions suffer from poor reliability fairness, while CSMA based solutions suffer from low channel access and energy consumption fairness.

In Chapter 7, we present a detailed analysis of our machine learning based MAC for dedicated IoT networks in realistic conditions. Due to the low computational capacities and the low energy consumption nature of IoT devices, we consider that the machine learning processing should be done at the gateway node. To do so, the gateway must obtain all necessary information to train the machine learning algorithm and continuously learn about the network behavior. The distance separating the device from the gateway is present in the algorithm input data in Chapter 6, while in a real situation it is hard to obtain the distance with a good accuracy. Instead, the node activity time is an information that the gateway is capable to measure, and we believe that the device activity time could present an indication about the distance between the gateway and the device. Therefore, we replace the distance in the input data by the device activity time. And, in order to gain a higher level of realism, we consider a heterogenous node deployment, instead of the uniform distribution previously used. The simulation results confirmed the conclusions of the previous chapter and brought promises of better performance without any hardware or structural changes, but only with adding learning capabilities in the way of accessing the channel.

2. State of the Art

The main contribution of this thesis is the application of machine learning techniques in order to propose a cognitive MAC layer for dedicated IoT networks. The dedicated IoT networks represent the main context of our work; we try through Section 2.1 to present an overview about this type of networks. Then, through Section 2.2, we give an overview on the MAC layer in this context, where we present the most used approaches. We also show, throughout Section 2.2, the main challenges that faces the MAC layer for different types of network and discuss some proposed enhancements in the literature. Finally, in Section 3.3, we briefly introduce the machine learning techniques, and then we show how machine learning in used in the networking field, starting by citing network security related contributions and ending by citing contributions at different architectural layers.

2.1 Internet of Things

The dedicated IoT networks come with the promise of connecting thousands of sensing devices to a same central gateway node. This is obtained with a one-hop star topology, in a coverage area ranging from 1 km to 10 km.

The number of applications based on IoT technologies is continuously increasing and they belong to many fields, such as smart homes, smart cities, security, industry and health monitoring. The essential requirements of an IoT application are long-range transmissions, large geographical coverage, low energy consumption with a battery autonomy that could reach 5 to 10 years, usage of cheap and small devices and communications that are optimized for very small data rates. Therefore, the usage of technologies with a short-range transmission, such as Zigbee and Bluetooth, is not adequate for dedicated IoT applications. Meanwhile, cellular communications offer long-range transmissions, but cellular network do not satisfy the low energy consumption requirement of IoT application.

In this context, the Low Power Wide Area Networks (LPWAN) have appeared with an architecture that satisfies all the IoT application requirements, as shown in Figure 2.1.

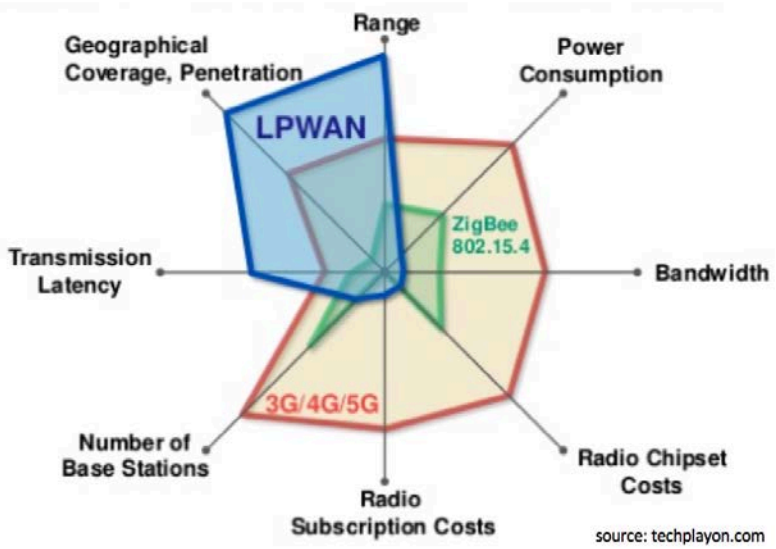


Figure 2.1: Comparison between LPWAN, a short-range technology (Zigbee) and Mobile networks [80]

The economic features of LPWAN in terms of energy consumption, device price, low-cost communication, and inexpensive deployment, made it reach high popularity in research and industry

fields. Two principal actors share the LPWAN market: SigFox and LoRa. The first one on the market was SigFox, a French society based in Toulouse launched in 2009. The second one was LoRa, an open-source protocol based on a proprietary modulation, which was initially developed in France by Cycleo, and later bought by the American society Semtech.

Although the market approaches of SigFox and LoRa are different, they remain pretty similar from a technical point-of-view. They both operate on the same frequency ISM (Industrial, Scientific and Medical) band; this frequency band is free and no need to pay for a license. However, this comes with a 1% time-on air limitation per node, in order to make the spectrum available for a large number of devices. This condition limits the throughput significantly, in the uplink for example, a maximum of 140 messages of 12 bytes that could be sent daily by a device in a SigFox or LoRa network. While, for the downlink, the data rate is very limited, 4 messages of 8 bytes per day for a SigFox network. Even though transmissions use public unlicensed bands, the frequency usage is regulated (ISM band 868 MHz in Europe, 902 MHz in USA) and the base frequency, as well as the authorized bandwidth, should respect local regulation of each country.

2.1.1 SigFox

SigFox is a system of wireless connections that uses radio frequency signals that are long range and ultrafast, known as Ultra Narrow Band (UNB). With a bandwidth of 48 kHz, and a central frequency of 862 MHz, in France and Europe, a SigFox device is capable to transmit during 30 seconds per hour. Transmissions with SigFox are done in “fire and forget” way: the sending device does not wait for any acknowledgement from the receiving station. The device has no prior knowledge of stations in his radio transmission area. Hence, the device sends each message multiple times: three transmissions for a same message, on three different channels. The device has to select transmission frequencies, while the reception frequency (in case of a downlink available) is the same as the one used for the last transmission.

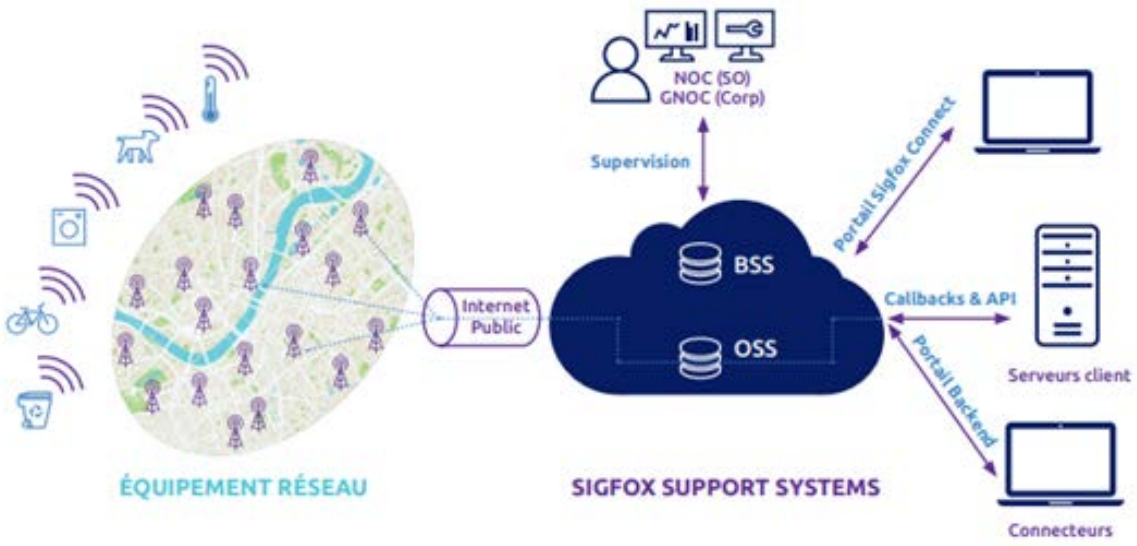


Figure 2.2 : SigFox Architecture [81]

The messages transmitted by the devices are received by a base station. Then, the station transmits those messages to the backend (BE) through an Internet connection, as illustrated in Figure 2.2. The BE stores the messages and sends them to the Information System (IS) of the client. The BE has the capacity to connect to a base station; however neither the BE nor the base station are able to connect to a device.

With more than 2000 antennas deployed by SigFox in France, the IoT network of the operator covers 94% of the French population. The French company is also present worldwide, in 70 countries. For 21 among them (30%), it has a coverage at the national level, such as in Belgium and Spain. In the United States, SigFox was covering the third of the population in early 2019. Recently, on March 12, the French IoT operator entered the Russian market and created the entity “SigFox Russie” with the Russian company Energo Capital. More than 1.1 billion persons in the world are able to take benefit of the IoT SigFox network. Figure 2.3 shows the IoT coverage targeted by SigFox for 2023.

Figure 2.3 : SigFox planned coverage for 2023 [82]

The economic model of SigFox is based on a subscription per connected device, while acting as a direct operator in France and the United States.

2.1.2 LoRa

LoRa, for Long Range, is a technology and a protocol developed by Semtech, based on a French technology developed by the Cycleo startup, and acquired by Semtech in 2012. The LoRa alliance was created in 2014 to support technical specifications.

LoRa MAC and LoRaWAN are the two successive versions of the protocol at the MAC layer. LoRa stands for the physical layer specifications, including a proprietary modulation, while LoRaWAN is the upper layer protocol on which LoRa operates and is maintained by the LoRa Alliance. At the physical layer, LoRa is based on transmission with wide spectrum and low amplitude, contrarily to SigFox where transmissions use Ultra Narrow Band with higher power.

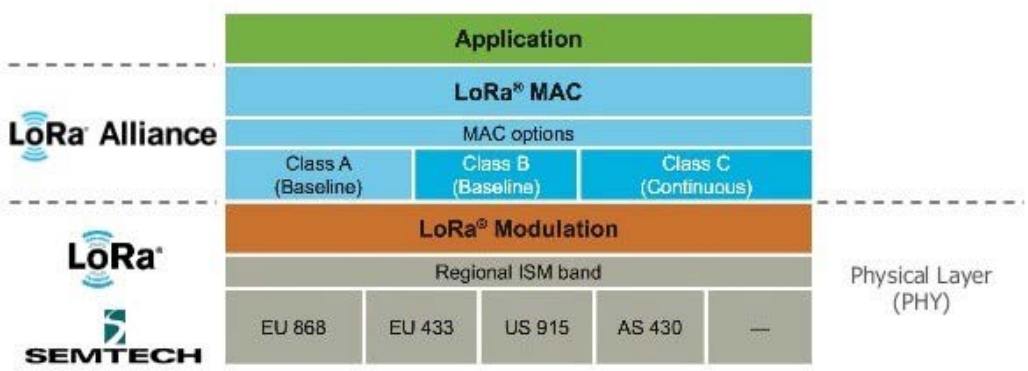


Figure 2.4 : LoRa protocol stack [83]

Three different classes of LoRaWAN devices exist: A, B and C. The device of Class A category are bi-directional end-devices, where a node can send a message anytime. Then, the device waits for an acknowledgement from the gateway after a certain time RxDelay1 or RxDelay2, as illustrated in Figure 2.5.

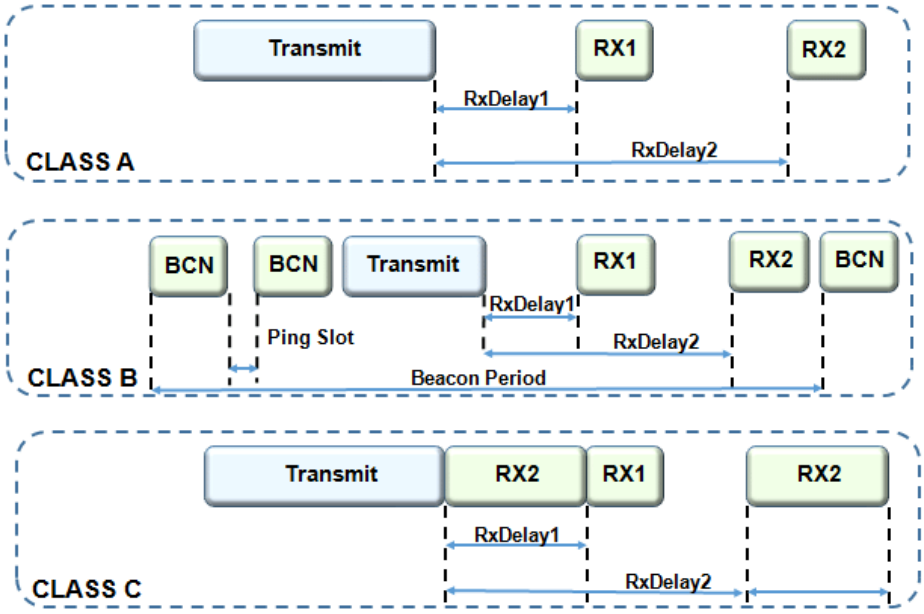


Figure 2.5 : LoRa device classes [84]

The Class B of devices is similar to the previous class, but the exchange is scheduled using beacon messages transmitted by the gateway. The device can receive multiple downlink messages in this case, as seen in Figure 2.5.

The Class C of devices extends the Class A, by making the devices keep their reception window open between two transmission. This class is more energy consuming than Class A, but still interesting for low-latency applications.

LoRa is based on its own modulation techniques, called Chirp Spread Spectrum (CSS), which assigns different spreading factors (SFs) to users in order to make them resilient to external interference. A spreading factor is the number of bits encoded per symbol, and 2^{SF} is the number of possible symbols per spreading factor. A chirp is a signal that continuously increases or decreases the

frequency over time. The chirps are cyclically shifted and the frequency jumps determine which symbol is encoded.

The SF represents the spectrum extension to transmit a message, for example higher SF allows to communicate over farther distances between the gateway and the device. However, this comes with the price of lowering the available bandwidth. Hence, for higher SF we cover larger areas but with lower throughput.

2.1.3 NB-IoT

Classical telecom operators, who propose data services (3G, 4G, etc.), have been competing since almost two decades to offer higher throughput. Nowadays, the 3G and 4G throughput allows to watch live videos on smartphones. Traditional mobile operators took time to get interested in LPWAN. In June 2016, the 3rd Generation Partnership Project (3GPP) announced the creation of NB-IoT, which is the new LPWAN communication standard proposed by telecom operators.

Narrow-Band IoT (NB-IoT) is an update of the current 4G (LTE), hence it has the advantage to offer a country-wide coverage. NB-IoT is based on the same principle as other dedicated IoT technologies: to offer a long-range solution, with low data rate and very low energy consumption. NB-IoT offers a throughput of 20 kbits/s, better than SigFox and LoRa. However, this comes with the price of higher energy consumption with respect to other dedicated IoT solutions.

NB-IoT can function in three different manners, illustrated in Figure 2.6. The first one is over the old GSM network, using the frequency band of 200 kHz. This frequency band is presently less used, which gives some space for the NB-IoT technology to offer an LPWAN solution. The second mode of operation is within the LTE network, with resources reserved for NB-IoT. Finally, the solution can be deployed in an independent NB-IoT network.

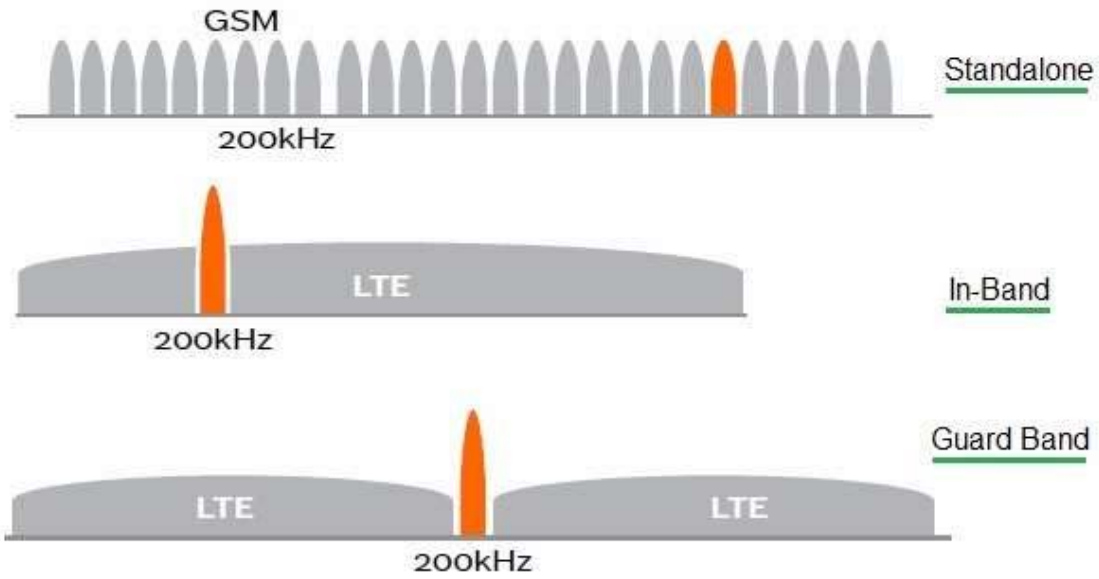


Figure 2.6: Frequency spectrums supported by NB-IoT [85]

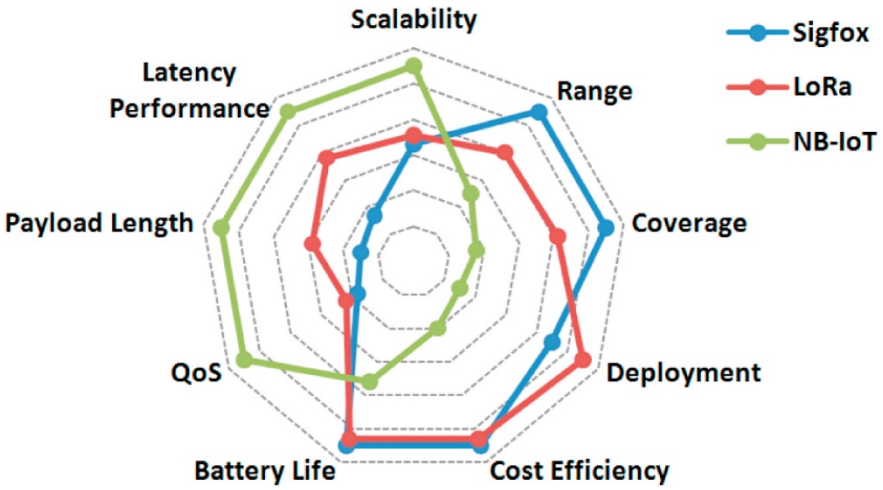


Figure 2.7 : Respective advantages of Sigfox, LoRa, and NB-IoT in terms of IoT factors [86]

In Figure 2.7, we present a comparison between the features of different dedicated IoT technologies. The NB-IoT technology does not meet the economic requirement of LPWAN as much as SigFox and LoRa in terms of power consumption and cost efficiency. However, NB-IoT offers a better quality of service and latency performance with respect to other IoT actors.

The NB-IoT market has known a fast growth. In 2019, more than 93 NB-IoT networks have been created by more than 50 different mobile operators. The leading player of NB-IoT is Huawei Technologies (China), and Vodafone Group, Emirates Telecommunications Corporation, Qualcomm and Intel Corporation are among the principal actors.

2.1.4 WiFi HaLow

The Wi-Fi Alliance is also an IoT actor, with its proposed IoT technology denoted as WiFi HaLow or IEEE 802.11ah. The WiFi-HaLow technology uses the frequency band under 1 GHz, which offers twice the range of classical Wi-Fi (which uses the bands 2.4 GHz and 5 GHz), consumes less energy and penetrates easier through walls and obstructions.

The HaLow standard satisfies all the dedicated IoT network requirements. Moreover, it has the advantage of adopting the existing Wi-Fi protocols, which offers simplicity of usage and interoperability. Therefore, future WiFi-HaLow routers will be capable to function in classical Wi-Fi bands and will be able to connect thousands of devices to one access point. The throughput offered for Wi-Fi HaLow connections will be between 15 kbit/s and 18 Mbit/s. However, this technology only recently arrived in the market and seems oriented towards indoor scenarios

2.2 Medium Access Control Layer

The Medium Access Control (MAC) layer plays the role of defining the rules of access to the medium. The medium is the object that the devices of the network use to communicate with each other. This could be a wire in the case of a wired network, while for a wireless network the medium is a shared frequency/channel.

We focus in our work on wireless networks, therefore, in this subsection, we focus on the principal MAC layer solutions for wireless networks, on the main challenges faced by the MAC layer for wireless networks, and on some proposed enhancements. Then, we present how the MAC layer

challenges are different for dedicated IoT networks and we disciss the presently used MAC layers by IoT providers.

One of the first MAC protocols is Aloha, which is a simple 50 years old medium sharing method, widely used in the networking domain. It was implemented at the beginning to connect the Hawaii university campus using ultra high frequency in a wireless topology, to ensure the connection between a central computer station and its scattered connected terminals in different Hawaiian Islands [33]. The Aloha MAC is technically very simple: when a device has a frame to send, it transmits it immediately without any coordination with other devices. Then, the receiver has to acknowledge the good reception, otherwise the sender retransmits the frame. This operation is repeated until the correct reception of the frame, otherwise the sender device drops the packet after a certain number of tentatives.

Another version of Aloha, called Reservation Aloha, has been introduced in the ‘70s for satellite communication links, because it allowed simple dynamic allocation of the channel [34]. The simplicity of the Aloha protocol made it gain popularity, and it is also used in mobile networks ever since their first generation, where the protocol use was limited to signaling messages. Nowadays, the latest mobile communication standards still use a MAC solution which is Aloha-based, consisting of a combination between slotted-Aloha and Reservation Aloha [35,36].

With the appearance of short range networks, such as Wireless Sensor Networks, where there is more vicinity between connected devices, the requirements for a good MAC protocol changed. For WSN, the radio transmissions, which are mainly controlled by the MAC layer, represent the principal source of energy consumption. Then, the MAC protocol should optimize the energy consumption by fighting against lost packets, which are caused by collisions, diminish the time to access to the channel, reduce the overhearing (i.e. reception of a message destinated for other device), control overhead and over-emitting (i.e. sending to a non-ready to receive device).

Then, the first idea to save energy is to turn off the radio transceivers when they are not used. This extends the autonomy of the device battery but brings synchronization challenges and regarding the distribution of the sleep/wake-up periods among devices. Therefore, the WSN dedicated MAC protocol should assure longer sleep periods for a device without affecting the communication. Many research works proposed MAC protocols for WSN, we distinguish two main categories: scheduled protocols and contention-based protocols.

2.2.1 Scheduled protocols

These protocols are very energy efficient, since they avoid collisions and overhearing. Scheduled protocols form clusters of nodes and communication inter-cluster is done through one of the following approaches: Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA) [70].

The FDMA for inter-cluster communication is efficient to reduce collisions, however this comes with the price of more energy consumption, since the FDMA usage imposes hardware modifications (additional circuits) in order to dynamically switch between radio channels. The CDMA shows a similar behavior, an efficiency in fighting collisions, but the required processing consumes a non-negligible amount of energy [71]. Finally, the TDMA MAC solution aims to optimize the slot attribution process in order to minimize the energy consumption. However, TDMA suffers from a scalability problem and from a lack of adaptability towards a topology change. Moreover, network devices depend on the distributed synchronization and their throughput is limited because of non-used listening slots.

Many contributions have been proposed in the literature in order to ameliorate these approaches. For example, Katayoun *et al.* [72], proposed a scheduled MAC they denoted Self-organizing Medium Access Control for Sensor Networks (SMACS). The authors present SMACS as a combination between TDMA and FDMA, where neighbor nodes choose randomly a link (a time slot and a frequency). This protocol improves scalability but requires important overhead.

2.2.2 Contention-based protocols

In this type of MAC protocols, the devices access to the channel during the same time interval, using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique. Many variants of the CSMA/CA technique exist, each one of them aims to avoid the collisions. The principal advantage of this type of protocols is the increased scalability compared to the scheduled approaches. However, when the network load is high, the CSMA/CA based MAC does not guarantee a fair access to the channel.

CSMA/CA is used by the standards in the IEEE 802.11 family [68], in which the sending device must sense the channel to be free before transmitting. In CSMA/CA, the collisions cannot be detected, which is the case with CSMA/CD (with Collision Detection) [73] wired networks. Hence, the device tries to avoid the collisions by avoiding to send a message unless the channel is free. Even when the channel is detected free, the sending device waits a random number of slots where the channel should continue to be free before initiating the transmission.

Wei *et al.* [74] proposed a MAC protocol based on CSMA/CA, they denote Sensor MAC (S-MAC). The proposed protocol uses the CSMA/CA access method where the connection between two devices is initiated by the exchange of control messages Request-To-Send (RTS) and Clear-To-Send (CTS). The protocol is conceived to offer a more energy saving access method for WSN. The authors show how this message exchange phase helps to avoid more collisions and resolves the problem of hidden nodes. In S-MAC, the device goes in a sleep mode for a certain period and wakes up for another period to sense the medium, and many devices can have the same wake up cycle. The devices broadcast their sleep/wakeup schedule to their one hop neighbors. Thus, every device has the information about when it can wake up to communicate with its intended receiver. With S-MAC, maintaining a good synchronization is necessary; this is done by making nodes send synchronization messages SYNC at the beginning of the wake-up cycle of their neighbors. Wei *et al*. explain that S-MAC is interesting for a certain number of applications, such as environmental monitoring, where sensors are inactive for long periods of time and wakeup only when something is detected. The S-MAC is conceived to maximize the life of the network, while other criteria are not considered, such as latency.

Van Dam *et al.* [75] propose a performance enhancement of S-MAC, denoted as T-MAC. The authors introduce an adaptive duty-cycle, by dynamically ending the wakeup period. With T-MAC, when the device is in wakeup cycle and does not receive a message after a certain period, it goes back to sleep. Thus, T-MAC minimizes idle listening of S-MAC. With experimental results, authors show how T-MAC and S-MAC obtain similar results under homogeneous network load, while for variable network load T-MAC is five times more performant than S-MAC. However, T-MAC makes the node sleep before making sure that any neighbor has a message to send, for example a channel access failure could cause a delay for the neighbor to send his message.

One of the principal approaches to reduce the idle listening is the Low Power Listening (LPL), where an inactivity period was added to the physical layer. The main idea is to make the sender device send long preamble message to its intended receiver. Then, the receiver should activate its radio periodically in order to detect the presence of a preamble. The transmission duration of a preamble should be equal to the duration between two wakeups of a receiver. Joseph *et al*. [76] propose one of the first MAC protocols for WSN which uses LPL, denoted as Berkley-MAC (B-MAC). Then, in [77], the authors propose an energy efficient MAC protocol based on synchronized preamble sampling, which they denote as Wireless Sensor MAC (Wise-MAC). Wise-MAC reduces the length of the preamble in function of the wakeup periods of the receivers. Michael *et al.* [78] proposed X-MAC, which decomposes the preamble into small size preambles. The proposed protocol has shown better energy saving results and lower latency with respect to traditional LPL protocols.

The Low Rate Wireless Personal Area Networks (LRWPAN) are also short-range networks where we use as MAC protocol CSMA/CA and slotted CSMA/CA. The CSMA/CA used for LRWPAN is a variant similar to the one used for IEEE 802.11 networks, but with reduced backoff, while slotted CSMA/CA uses super-frames that aim to synchronize the connected devices and reduce

the energy consumption of each device. The synchronization is also done with the transmission of beacon messages. Afterward, the Contention Access Period (CAP) starts, which allows every device to send and receive frames with the CSMA/CA mechanism. However, CSMA/CA induces important energy consumption, especially during loaded traffic, which led the authors of [79] to reduce the backoff and hence reduce the period of contention (the time spent by sender nodes listening the channel before transmission).

2.2.3 MAC protocols for dedicated IoT networks

Dedicated IoT networks are long range networks, with different requirements compared to the short range networks discussed above. Through this subsection, we present the MAC protocols used by the main dedicated IoT providers.

SigFox and LoRa both use an Aloha-based MAC solution, hence when a device has a message to send it can freely access to the channel. Meanwhile, NB-IoT uses Single-Carrier Frequency Division Multiple Access (SC-FDMA) for the regular uplink transmissions and slotted Aloha for the resource reservation process.

LoRa uses an Aloha MAC protocol while adding a frequency diversity, with the use of three channels inside the ISM band, with a width of 125 kHz. The channels are 868.10 MHz, 868.30 MHz and 868.50 MHz in Europe. On these frequencies, LoRa transmissions are limited by regulations to a 1% time-on-air. LoRa offers a dynamic data rate, which highly depends on the spreading factor (SF) and on the used modulation.

The MAC layer of SigFox is based on Aloha and it transmits 3 frames for the same packet. The transmission frequency is chosen randomly in a macro-channel of 200 kHz inside the ISM band. SigFox uses an UNB binary phase shift keying (BPSK) modulation on several channels.

The dedicated IEEE standard for IoT, WiFi HaLow, uses a CSMA-based MAC solution. This standard is intended to be the MAC layer solution for indoor IoT networks. The only modification with respect to CSMA/CA is the division of the connected devices into groups and the channel access is restricted to devices belonging to one group at a given period of time.

Surprisingly, all dedicated IoT technologies, use classical MAC solutions and none of them takes advantage of recent MAC enhancements and innovations, such as those proposed in WSNs. Only a few modifications are done, for example in the case of SigFox with the use of pure Aloha over multiple channels, or for LoRa with the use of an orthogonal coding scheme. Finally, Wi-Fi HaLow keeps the same basics principles of the CSMA protocol, while diving colliding devices into groups.

Aloha is the most used MAC protocol in an IoT context, and that is due to its simplicity, which perfectly fits the low computational capacities of IoT devices. However, this protocol has a well-known scalability problem, which is a main requirement for IoT networks. CSMA is less popular currently, but it also presents a scalability problem after a certain density and it does not guarantee fair channel access to devices.

Several studies have been conducted in the literature in order to propose new MAC solutions for dedicated IoT networks, without the limitation of classical MAC approaches. Some research work focused on adding the CCA mechanism of CSMA to pure Aloha for outdoor IoT networks [60]. Other works proposed a persistent-CSMA based MAC layer for IoT networks [63]. However, these contributions did not consider the low sensitivity of IoT devices and supposed that each device is capable of hearing all its contenders, which does not seem realistic. There are also contributions, where a coexistence between CSMA and Aloha is studied for dedicated IoT networks [62]. However, the results were not very promising, and important unfairness between Aloha and CSMA devices was observed.

Meanwhile, our strategy to enhance the MAC layer for dedicated IoT networks is to use cognition capacities instead of using static approaches. This allows the IoT network to take advantage of the strengths of both MAC protocols, Aloha and CSMA. To the best of our knowledge, this contribution is the first to use machine learning at the MAC layer for LPWANs. However, other

machine learning based MAC solutions have been proposed for other types of networks. We present some of them in the following section.

2.3 Machine learning

The machine learning techniques appeared in the middle of the previous century, and the application of machine learning has been increasing since early 1980's [1]. The machine learning application area covers from a simple house price prediction to alerting about a serious health problem. In the networking field, machine learning approaches have been discussed in the literature in order to solve many network issues such as security, or even to enhance the network performance.

Network security was among the first networking domains where machine learning was used. Sinclair *et al.* [2] used a combination of machine learning techniques to develop a network security solution based on a genetic algorithm and decision tree. The authors prove how their machine learning based solution helps to differentiate anomalous connections from normal network connections. Shon and Moon [3] also proposed a machine learning algorithm that classifies abnormal behavior in the network. They apply a hybrid machine learning technique, which is a combination of supervised and unsupervised Support Vector Machine (SVM), denoted enhanced SVM. The authors explain their choice by the difficulty of using unsupervised SVM in a real application, due to the high false positive rate. The paper results show how the use of enhanced SVM along with the unsupervised SVM approach increases the accuracy.

Machine learning techniques have been widely used in the cognitive radio field as well. Mahonen *et al*. [4] present a solution to avoid harmful interaction between competing technologies using the unlicensed ISM band. The authors propose a Cognitive Resource Manager (CRM) which performs a cross-layer optimization with the use of machine learning algorithms, such as clustering and neural networks. Clancy *et al*. [5] propose a machine learning based solution for cognitive radio systems. The paper contribution consists of developing a framework that uses learning techniques along with reasoning techniques. The authors address two common problems in cognitive radios: capacity maximization and dynamic spectrum access.

Alsheikh *et al*. [6] provide an extensive review over the period 2002-2013 regarding machine learning applications in WSN. The authors present different WSN challenges, as well as the different machine learning based solutions proposed in the literatures. The authors analyze each solution and give its pros and cons. The discussed problems are security issues, routing problems and medium access control.

Yi *et al*. [88] proposed an enhancement to slotted-Aloha based MAC solution for WSN using Q-learning. Q-learning is a reinforcement learning technique, where the system takes different states and an action needs to be taken at each state. This technique is used here to find the $Q(i,k)$, which indicates the action that *node i* will take in slot k. Afterward, the Q-learning approach orchestrates the active/sleep cycle of the device by making receiver nodes wake up only during preferred slots of their transmitter nodes, a procedure denoted by the authors as informed receiving method. When a sender node reaches its preferred slot and has no message to transmit, it informs the receiver node by sending a ping packet. The authors show, with simulation results, how the Q-learning technique helped to considerably reduce the idle listening and overhearing, thus avoiding useless energy consumption, while achieving over twice the throughput of a pure slotted-Aloha.

Mario *et al*. [89] propose a dynamic CSMA protocol for WSN, where some CSMA protocol parameters are adjusted with a fuzzy logic controller. The fuzzy controller collects network performance data such as throughput and workload, in order to adjust the contention window size and the backoff exponent of the CSMA protocol. The authors show through experimental results the improvement obtained for the packet loss ratio and the throughput/workload ratio. However, experiments were conducted under low dense network, only 7 sender nodes and one gateway, in a one-hop topology, which cannot be considered a representative scenario for WSNs.

Jiang *et al*. [7] reviewed the benefits of machine learning application in wireless systems. The authors introduced some of the main machine learning algorithms and discussed the best utility of each algorithm for the next generation networks. The machine learning applications presented in this work are mostly radio-related applications, focused on physical layer issues.

Imen *et al*. [87] proposed an enhancement to the CSMA/CA based MAC used in WSNs. The contribution is also based on the use of a fuzzy logic controller. The proposed approach consists of giving more priority to nodes that drop more packets from their queue and consumes more energy. In other words, giving more chances to the nodes that are discriminated from accessing the channel, or disconnected nodes. The fuzzy system takes as input the queue length and the traffic rate and, based on predefined fuzzy rules, the backoff exponent of each node is calculated. The authors show through simulation results that the dynamic adjustment of the CSMA/CA parameters reduce the energy consumption and the delay, and offer an improvement to the throughput and the packet loss ratio with respect to the classical CSMA protocol.

Kibria *et al*. [8] discuss the use of data-driven wireless network models for the next-generation networks. The authors show a set of network designs and optimization schemes using advanced data analytics, machine learning and artificial intelligence. They present also the different challenges and concerns of deploying each of the aforementioned techniques. One of the main challenges is to manage the leverage of massive amount of data, while the prime concern is still non-technical: the operators are not ready to lose direct control over the network.

Several studies have been conducted in the literature focused on the impact of using machine learning techniques at the MAC layer. Doerr *et al*. [9] propose the MultiMAC framework for cognitive radio networks, that switches intelligently between different MAC solutions. The authors introduce the MultiMAC as a mediating MAC layer in which we can put the implementation of several MAC solutions. They show through experimental results when the switch between different MAC solutions can be beneficial, based on the noise level. The experimental setup includes only two base stations and one noise generator. The contribution does not consider any acknowledgement messages and no frame retransmissions, and the context is different from ours, using big data payloads.

Sha *et al*. [10] propose a self-adapting MAC layer for wireless sensor networks. The authors develop a new MAC layer architecture that mainly uses automatic classification, in order to choose the optimal MAC protocol to use. The classifier uses the traffic and the noise level as entries to make a decision. The different MAC solutions to select from are placed in a MAC container. The experimental results in [10] show how the proposed self-adapting MAC solution satisfies all the application requirements in term of packet success ratio and energy consumption. However, the context of the study is only limited to WSNs, besides the fact that the proposed solution requires major modification to the MAC layer structure. Plus, the fact of incorporating many MAC protocol implementations in WSN devices could be non realistic because of memory concerns.

Rajab *et al*. [11] discuss the problem of standard coexistence in a same wireless network. The authors focus on the inter-standard interference, especially standards working under the unlicensed ISM band. They propose a MAC technology identification solution that uses different energy detection techniques, as well as machine learning algorithms, such as KNN and Naive Bayes. The authors prove the accuracy of their identification methodology through implementation of different versions of the IEEE 802.11 standard under homogeneous and heterogeneous network conditions. However, the contribution of the paper [11] stays limited to cross-standard interferences.

Bilal *et al*. [12] propose a machine learning based approach that selects the optimal MAC layer for IPv6 over Low Power Personal Area Network (6LoWPAN). The authors define the optimal performance as the highest throughput and the minimum latency. The CSMA protocol is the single MAC protocol present in the study and the optimization is obtained by changing the value of some CSMA parameters that fit the actual network conditions, in order to provide the best performance. However, the study is limited to 6LoWPAN, which is very different to our network nature. Moreover, the CCA threshold was not mentioned in the study, while we strongly believe that the CCA threshold

is among the most important CSMA protocol parameters. The results were limited to 50 and 100 nodes and the simulation was done with Matlab.

The aforementioned studies were done for different contexts than the dedicated IoT networks, hence the challenges and the evaluation metrics were different. For example, none of the previously mentioned contributions studied the impact of disabling the acknowledgement messages or tuning the CCA threshold value for the CSMA protocol. Moreover, big changes to the MAC layer architecture were introduced in many contributions. We believe that the development cost of these solutions can be a blocking point for their implementation for a real scenario.

3. Performance Evaluation of Channel Access Methods for Dedicated IoT Networks

The objective of this chapter is not to study the specificities of each of the technologies specified in the introduction chapter. Instead, we want to focus on the basic properties of the Aloha and CSMA/CA access strategies, in order to understand whether one of these solutions is more appropriate than the other in the IoT context.

As a matter of fact, Aloha and CSMA/CA have been well studied and compared in the literature, starting from the ’70s [20] and until the modern days [21]. However, the performance of the two schemes is generally evaluated in terms of throughput, while considering stations with saturated traffic. This is normal in local area networks, where the objective is to have a reliable and rapid communication, generally in terms of file transfer.

However, IoT scenarios are very different from this point of view, characterized by dense networks with sparse, unsaturated traffic. The classic use-case in these networks is data collection, where measures of some physical phenomenon (e.g. air pollution [22] or vehicular traffic [23]) are uploaded to a central server. In this case, the throughput is no longer an essential metric, as the performance of the IoT applications is much better described by metrics such as the packet reception ratio.

Indeed, Aloha and CSMA/CA are among the first MAC protocols to be proposed in the history of wireless networks. As a consequence, they have been thoroughly studied and compared in the last four decades [20]. However, despite considering the impact of numerous parameters, such as the buffer size [24] or the number of retransmissions [25], most of these studies focused on scenarios with saturated stations, i.e. users who always have packets to transmit to one another. This is quite different, both in terms of system functioning and metrics, from the dedicated IoT networks that represent the object of this thesis.

While new theoretical tools, e.g. based on stochastic geometry [17], were developed recently, the studied scenarios remained generally the same. Even in the few studies where Aloha and CSMA/CA were compared in scenarios with unsaturated traffic [26], the system throughput was still used as the main metric. On the other side, in the cases where an evolution can be noticed in terms of the studied metrics (e.g. the distribution of the channel access delay [27]), saturated traffic is considered. In related fields, where new wireless network architectures are imagined, e.g. in mobile ad hoc networks [28] or in vehicular networks [29], Aloha and CSMA/CA are always among the first MAC solutions to be tested. However, these studies remain focused on throughput in saturated traffic conditions.

Regarding dedicated IoT networks, two recent studies [30, 31], evaluate the performance of Aloha-based techniques. Li et al. [30], take a stochastic geometry approach, focusing on throughput and on the outage probability of a station, defined as the probability that a station observes a signal to noise and interference ratio (SINR) above a certain threshold. Song et al.[31], argue that packet delivery ratio is a more suitable metric in IoT use-cases, and they study the performance of slotted-Aloha with respect to this metric. However, the only parameter considered in [31] is the packet arrival rate. Most of these studies focus on analytical models, which are essential tools in the understanding of a network protocol. However, this type of mathematical modeling usually requires some important simplifications: e.g. the use of slotted-Aloha instead of Aloha [31], independence of retransmissions [28], or simplified CSMA/CA back-off [21].

In this chapter, we focus on these IoT metrics, through an extensive simulation study. We compare classic Aloha and CSMA/CA , showing that each of them is adapted to certain IoT scenarios and metrics. Furthermore, we evaluate the LPWAN flavor of Aloha, which does not employ ACKs. Interestingly, our results show that removing ACKs does not only conserve energy, but it can even improve the packet reception probability. Finally, for the first time in the

literature, we apply the same concept, the one of removing ACKs to CSMA/CA, showing interesting performance gains.

3.1 Simulation Methodology

Throughout this thesis, we use the Network Simulator 3 (NS3) to study a dedicated IoT network with N sender nodes and one sink node. The network topology is a circle with radius r and the base station sink node is its center, while the sender nodes are uniformly distributed inside this area and they all share the same channel. Each sender node produces one packet of data each time period T, while the sink node only transmits ACK frames (in case the MAC protocol uses them).

Different IoT technologies achieve very different data rates at the physical layer, from 100b/s in Sigfox to several Mb/s in WiFi HaLow. In order to have a fair, but technology agnostic comparison, we are using as a parameter the transmission opportunity, defined as

$$T_{op} = \frac{S}{T}$$

where S is the airtime of a MAC layer frame.

As an example, a T_{op} value of $165\ 10^{-6}$ corresponds to a packet arrival every second in WiFi HaLow and to one every 20 minutes in SigFox. As explained, unlike previous studies, which mostly focus on the throughput as an evaluation metric, we use metrics more relevant for the IoT context. To assess the network reliability, we use the packet success probability as a metric. We are also interested in energy consumption an important performance criterion in IoT networks, often battery powered. However, measuring the node energy consumption requires energy specific (or even hardware-specific) energy models. Therefore, trying to be energy agnostic, we measure the time each node spends in an ON state (receiving, transmitting or listening to the channel). We consider that this second metric is a good generic proxy for the energy consumption of a node.

To simulate the CSMA/CA protocol, we used the ns3 AdhocWifi-Mac as a MAC layer model, with the parameters indicated in Table 3.1. Since NS3 does not directly provide an Aloha implementation for radio networks, we adapted the same AdhocWifiMac model used in the CSMA/CA case. This allowed us to have the same basis implementation for the two solutions, for a fair evaluation.

The first adaptation required in order to model Aloha was to deactivate the clear channel assessment (CCA) mechanism, which implements the carrier sensing operation. Since Aloha does not use carrier sensing, we set the CCA threshold to an infinite value, so that the node always considers the channel as free and the transmissions are never blocked. Another adaption consists in deactivating the random back-off used in CSMA/CA before a new transmission; we do this by setting the maximum contention window to 0 in AdhocWifiMac.

We run simulations while varying the number of sender nodes. Every simulation lasts 30 seconds and it is repeated 10 times, with a different seed value each time. All the results presented in the remainder of the paper are shown with a confidence interval of 95%.

Parameter description	Value
Acknowledgement Timeout	75 ms
Maximum Number of Retransmission	7
RTS/CTS message exchange	Disabled
Frequency	5.180 GHz
Transmission Power	16 dBm
Clear Channel Assessment Threshold	-99 dBm
Propagation Loss Model	Log Distance
Propagation Delay Model	Constant Speed Model
Transmission Data Rate	6 Mbps
Transmission Opportunity	165 10^{-6}

Table 3.1 : Simulation main

3.2 Aloha and CSMA/CA Comparison

We begin our study by comparing the classical Aloha and CSMA/CA solutions in a dedicated IoT context. We evaluate the packet success probability and the time spent by the nodes in an active ON state, while also looking at the impact of the number of authorized retransmissions.

3.2.1 Packet Success Probability

The essential performance metric in IoT networks is the success probability of a message. The small size of the messages transmitted by the nodes allows their encapsulation into single packets, which are possibly transmitted multiple times as MAC layer frames.

Since we are interested in the overall performance of the MAC layer, in Figure 3.1 and Figure 3.2 we present the average packet success probability of the two MAC protocols studied in this section, calculated for different number of contending nodes and packet arrival periods (expressed in terms of transmission opportunities, T_{op}).

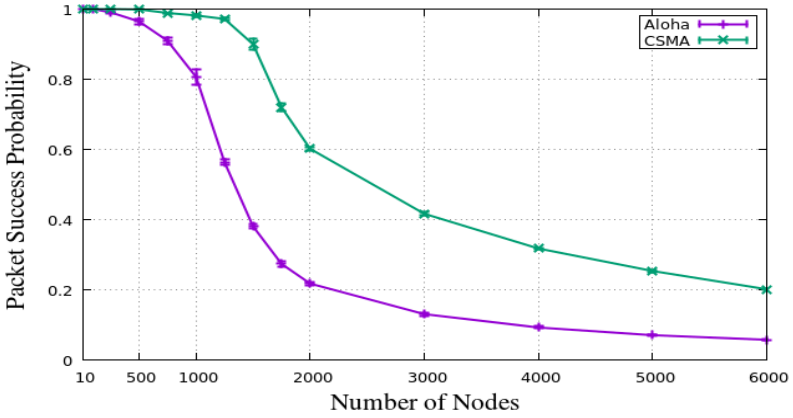


Figure 3.1: Packet success probability for Aloha and CSMA/CA when $T_{op} = 165\ \ 10^{-5}$

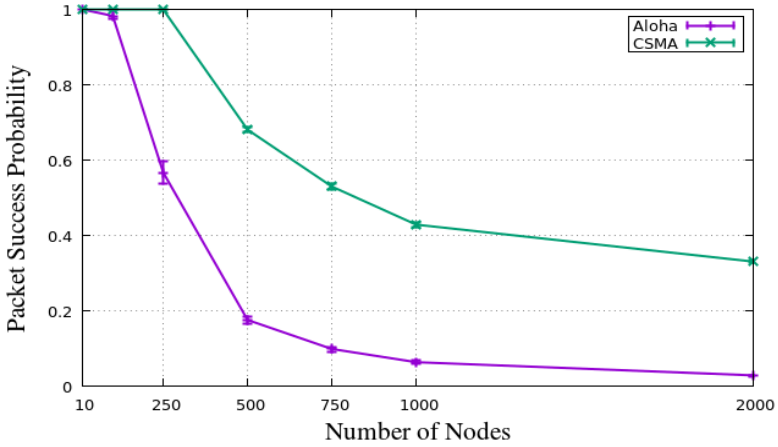


Figure 3.2 : Packet success probability for Aloha and CSMA/CA when $T_{op} = 165\ \ 10^{-5}$

In Figure 3.1, showing the packet success probability obtained for a transmission opportunity $T_{op} = 165\ \ 10^{-5}$ and for different number of nodes, we can distinguish two different regions. In the first region, for small networks up to 100 nodes, the CSMA/CA and Aloha success probabilities are both equal and near to 1. In the second region, for medium size and dense networks, the performance of the two protocols starts decreasing, with CSMA/CA getting the best results. This is expected, as CSMA/CA is using a CCA mechanisms to reduce the number of collisions and a back-off technique to avoid their repetition.

To complement these results, we also show the packet success probability for a transmission opportunity value ten times smaller in Figure 3.2. This corresponds to scenarios with a more reduced packet arrival rate. A similar trend can be observed, but the capacity of the network, in terms of number of nodes, increases.

3.2.2 Node ON Time

The energy consumption is an important metric for most IoT devices, constrained in terms of size, hence battery. As explained above, in this work, we do not directly compute the node energy consumption, as this would limit us to the numeric values of a particular technology. Instead, we calculate a correlated metric: the duration each node spends in an ON state, i.e. the time the node is using its radio module, either for transmission, reception or listening the channel.

In the case of Aloha, we consider that the node is continuously listening the channel while waiting for an ACK message. In the case of CSMA/CA, we consider that the node is ON to sense the channel during the back-off slots and after the transmission, listening to the channel waiting for an ACK message.

Figure 3.3 and Figure 3.4 (please note the log scale of the axes) show the average ON time for the two protocols, for two values of the transmission opportunity parameter and for different number of nodes. We observe that, for a low density network, both protocols have almost the same energy consumption, because we are not facing any collision or CSMA/CA back-off yet. Interestingly, as the number of nodes increases, CSMA/CA becomes more energy-friendly than Aloha for a while, since the latter solution results in more collisions and therefore requires more retransmissions. However, after a certain threshold, Aloha demonstrates a much better performance, consuming 10 times less energy than CSMA/CA. This trend is observed for both values of T_{op}.

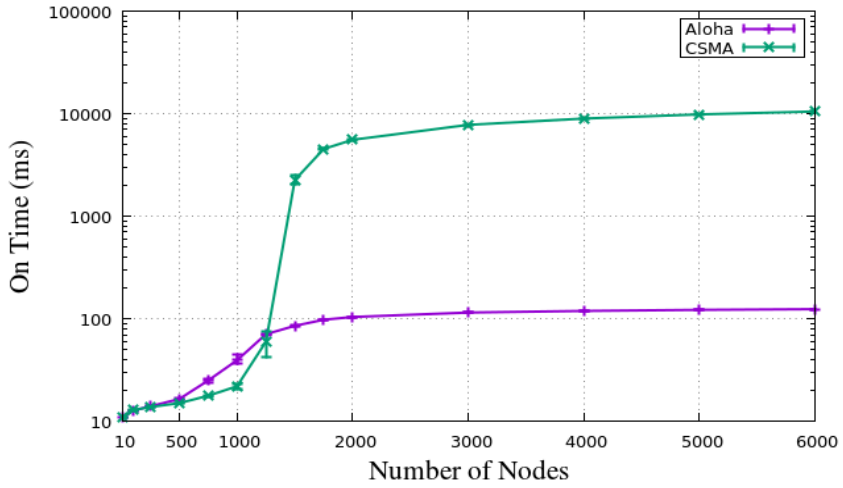


Figure 3.3 : Average ON time for Aloha and CSMA/CA when $T_{op} = 165\ 10^{-5}$

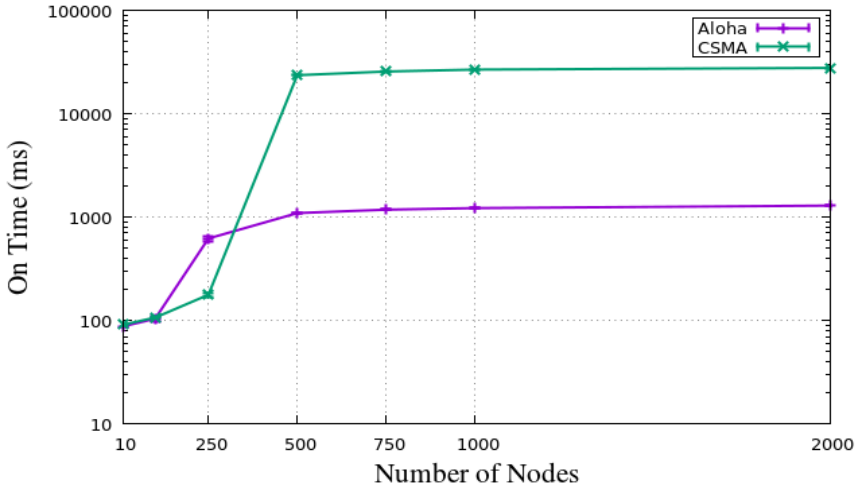


Figure 3.4 : Average ON time for Aloha and CSMA/CA $T_{op} = 165\ 10^{-6}$

3.2.3 Impact of the Number of Retransmissions

Both CSMA/CA and Aloha use back-off-based retransmissions in case of a missing ACK. In CSMA/CA, the re-transmissions follow a binary exponential back-off, which increases for each missing ACK. When the maximum number of retransmissions R is reached, the message is dropped and the packet is considered as lost.

We simulated Aloha and CSMA/CA with a maximum number of retransmissions of 3, 5 and 7, while keeping the other default MAC layer parameters from Table 3.1. Figure 3.5 shows the packet success probability with a variable maximum number of retransmissions, showing the significant impact of this parameter. For Aloha, we notice that the lower the number of retransmissions, the better the performance of the protocol. This is because a higher number of authorized retransmissions increases the collision probability. Aloha is also obtaining the best energy consumption results with the lowest number of retransmissions, as shown in Figure 3.6.

For CSMA/CA, the results are more mitigated: the packet success probability first decreases with R, just as in Aloha, but it then increases again (CSMA/CA with *R*= 7 gives the best performance in Figure 3.5). This is the consequence of two opposite behaviors: the increased overall collision probability with more retransmissions and the binary exponential back-off which reduces the collision probability for higher retransmission indices.

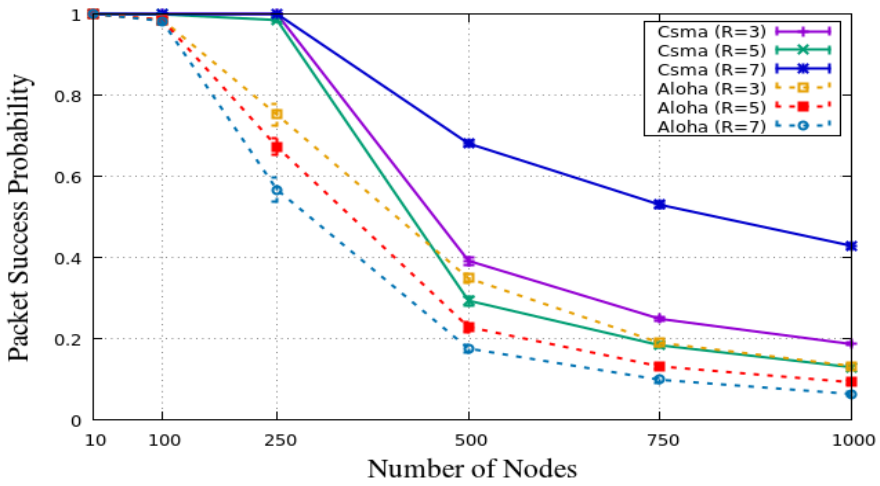


Figure 3.5: Packet success probability as a function of the maximum number of retransmissions in Aloha and CSMA/CA

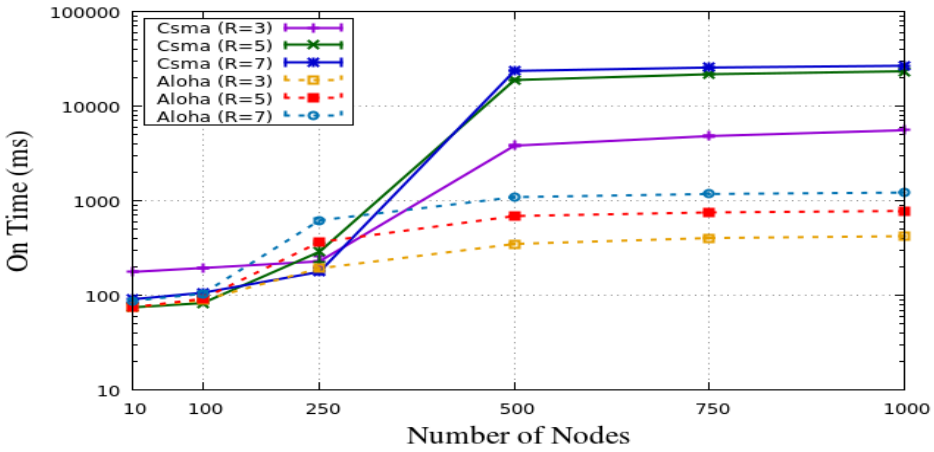


Figure 3.6 : Node ON time as a function of the maximum number of retransmissions in Aloha and CSMA/CA

We can see as well that CSMA/CA is obtaining better results than Aloha almost all the time in terms of reliability. This comes with an energy price, as CSMA/CA consumes more energy in networks of more than 250 nodes and this energy consumption increases with *R* (please note the log-scale on the y-axis in Figure 3.6). However, we still observe that CSMA/CA energetically outperforms Aloha for networks of 10 to 250 nodes.

From all these results, we can conclude that the best choice between Aloha and CSMA/CA in an IoT context depends on the metric we want to satisfy: Aloha gives better results energy-wise, while CSMA increases the packet success probability. The environment, e.g. the number of nodes and the packet arrival rate, also plays a major impact on the protocol choice, and so are the different parameters of the two protocols (maximum number of retransmissions, back-off mechanism).

3.3 Aloha without Acknowledgement Messages

As explained above, Aloha has been adapted to LPWAN technologies by removing the ACK messages. This mainly comes from a limitation of LPWAN solutions, where a down-link is not always available [13]. Instead, for reliability reasons, K copies of each message are transmitted by the nodes.

In this context, we study the impact of the absence of ACK messages, as well as that of the number of transmitted copies K, on the network performance. For this, we simulate a modified version of Aloha, under the same conditions as the previous simulations. This modified Aloha version, which we denote as **Aloha No Ack** in the remainder of the thesis, transmits each packet K times at the MAC layer, without waiting for any ACK message. For example, Sigfox currently uses a static value for this parameter in their system, K=3. To summarize, for the case when K= 1, the node sends the packet only once and goes back to sleep. For the case when K >1, the node wakes up and sends the packet once, and then sleeps a random number of slots before waking up again to send the next copy of the packet.

Figure 3.7 and Figure 3.8 show the results of transmission reliability and energy consumption obtained when comparing Aloha No Ack and classical Aloha. We remark that removing the ACK messages is not only a necessity to cope with a missing or limited downlink, but it actually improves the packet success probability. Indeed, Aloha No Ack with K= 3 is outperforming all the other Aloha and Aloha No Ack flavors in terms of reliability, as shown in Figure 3.7.

On the energy consumption side, Aloha No Ack has a constant ON time, which only depends on the number of transmitted copies K and it can be computed as $K \cdot S$. The results in Figure 3.8 show that Aloha No Ack with K= 3 consumes more energy than classical Aloha for a network with less than 250 nodes, but it outperforms the ACK-based approach for denser networks.

We note that ACK messages are generally considered as a prominent mechanism for reliability purposes at the MAC layer. In any throughput-focused solution, ACKs represent an essential feed-back to the transmitter. However, the results we obtained in this section demonstrate that removing ACKs actually brings benefits in IoT networks, when focusing on metrics such as packet success probability and energy consumption.

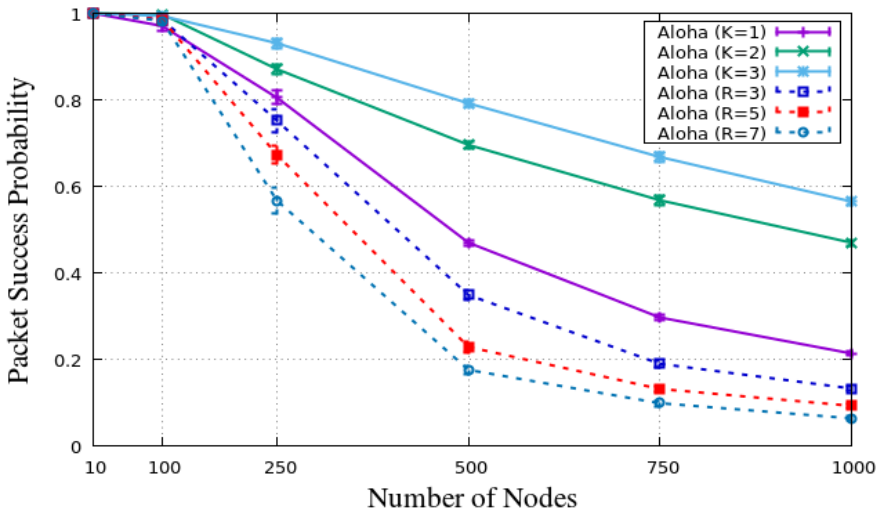


Figure 3.7 : Packet success probability for Aloha and Aloha No Ack

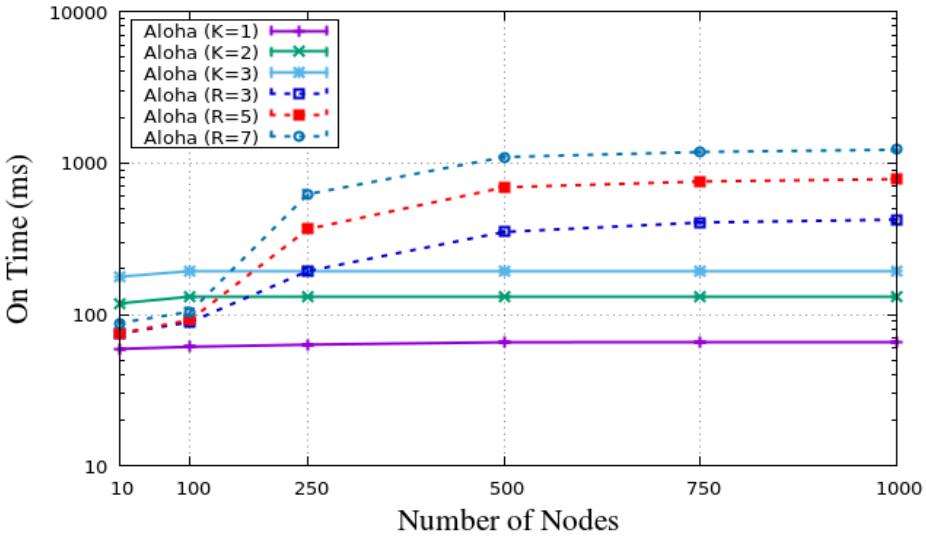


Figure 3.8 : Average node ON time for Aloha and Aloha No Ack

3.6 CSMA/CA without Acknowledgement Messages

Similarly, to how Aloha has been adapted for LPWANs, we propose removing ACKs from CSMA/CA as well. This solution, similar to what is used to transmit broadcast traffic in WiFi networks [20], has not been priorly tested in IoT scenarios before this thesis. Several studies conducted in parallel to our work, proposed adding carrier sense capabilities to LoRa devices, demonstrating significant gains. In our case, we take generic approach, focus on the mechanism itself, and not on a precise technology. In this solution, denoted as CSMA No Ack, we use a similar parameter as in Aloha No Ack for the number of transmitted copies, *K*.

Practically, a node wakes up to transmit a copy of the message and follows the CCA procedure. If the medium is detected as busy, the node transmits at the end of the back-off procedure. In order to transmit the next copy of the message, the procedure is repeated. However, in order to avoid repeated collisions, a back-off procedure is needed between the transmission of two copies. Since no ACK messages are used, the contention window used by the back-off mechanism, denoted as CW, cannot be dynamically adapted.

In Figure 3.9 and Figure 3.10, we compare the performance of the classical CSMA/CA and the modified CSMA No ACK version. For the packet success probability, shown in Figure 3.9, classical CSMA/CA obtains better performance for a network with less than 250 nodes. When the network density increases, we observe a phenomenon similar to the Aloha case: removing the ACK messages actually reduces congestion on the channel and allows CSMA No Ack to obtain up to 20% better performance than classical CSMA/CA.

On the energy side, in Figure 3.10, CSMA No Ack has an almost constant behavior: the slight increase one can notice for CSMA No Ack with K= 1is a consequence of the longer time required by the back-off procedure under high network density. On the other side, the classical approach shows a significant energy consumption increase in dense networks, where more retransmissions are needed. An important parameter for CSMA No Ack is the size of the contention window, CW, used between the transmission of two message copies. Figure 3.10 shows the impact of this parameter on the active ON time of a node, for K= 2. Basically, the higher CW, the higher the node ON time and the higher its energy consumption.

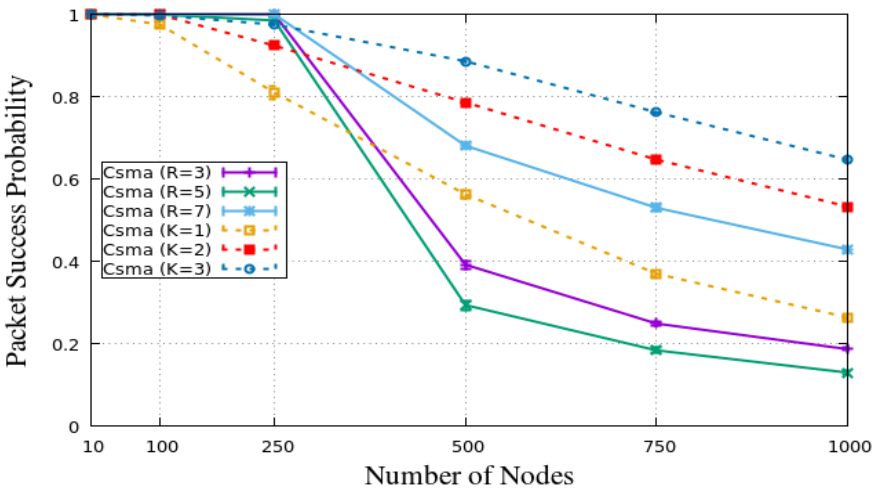


Figure 3.9 Packet success probability for CSMA and CSMA No Ack

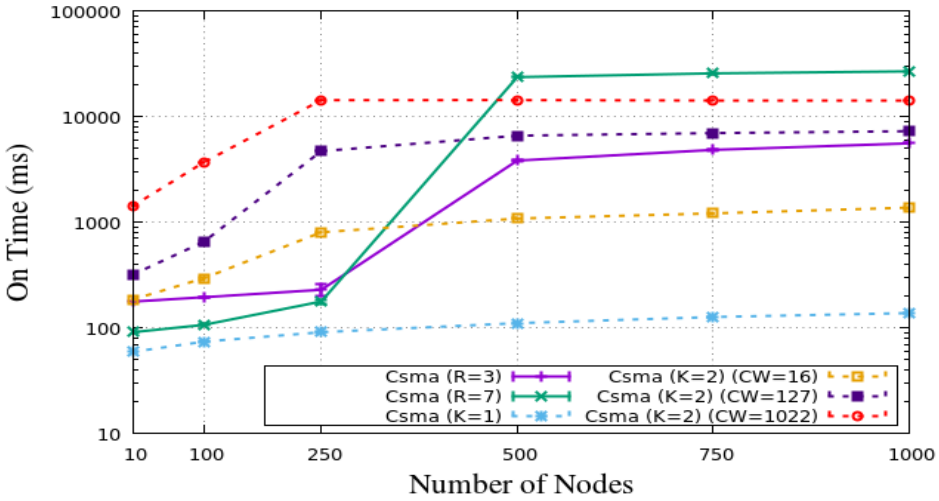


Figure 3.10 : Average node ON time for CSMA and CSMA No Ack

3.5 Conclusion

In this chapter, we discuss MAC layer solutions for dedicated IoT networks and evaluate them through ns3 simulation. We show that the best MAC layer approach depends on parameters such as the number of competing nodes and the packet arrival rate. In addition, we remark that using ACK frames can have a negative impact, always reducing the network performance in terms of reliability and energy consumption. This supports our belief that the MAC strategy for dedicated IoT network needs to adapt to the network state and to the target metric. Moreover, depending on the local traffic density, different MAC solutions can be used in different parts of the cell, orchestrated by a smart gateway. We explore such approaches the following chapters.

4. Analytical Study of Aloha without Acknowledgement Messages

The Aloha MAC protocol is a simple 50 years old medium sharing method, widely used in the networking domain. It was implemented at the beginning to connect the Hawaii university campus using ultra high frequency in a wireless topology, ensuring the connection between a central computer station and its scattered connected terminals in different Hawaiian Islands [33].

Another version of Aloha, called Reservation Aloha, has been introduced in the 70s for satellite communication links, because it allowed simple dynamic allocation of the channel [34].

The Aloha protocol is also used by the mobile networks ever since their first generation where the protocol use was limited to signaling messages.

Nowadays the latest mobile communication standards still use a MAC solution which is Aloha-based, consisting of a combination between slotted-Aloha and Reservation Aloha [35-36].

Since the appearance of the Aloha technique, many works have been conducted in the literature to study different Aloha flavors analytically [36-38], or even to propose some enhancements of the global performance, and mostly of the throughput[38, 39, 42-44].

For example, in [39], Raychaudhuri et al. propose an adaptive backoff mechanism to replace the exponential backoff used by default by the Aloha protocol and they prove the superiority of their solution analytically for an example of a satellite channel, in terms of throughput and delay.

Most of these works are limited to the slotted version of the protocol. The acknowledgement messages, the retransmission with a certain maximum limit and back-off mechanism are taken into account in the mathematical model, which increases the accuracy of these models. However, this also renders them more complex, so many of these works consider a saturated traffic in order to simplify the modeling work.

All the previously mentioned studies have considered an Aloha protocol with acknowledgement messages. Instead, we are interested in an Aloha version without the use of acknowledgement messages. In the previous chapter, we have shown the benefits of disabling these control messages on the packet success probability and on the energy consumption. This advantage of Aloha No Ack in IoT networks motivates us to provide a mathematical model of Aloha where no acknowledgement messages are used in the network.

Very few studies have been conducted on Aloha No Ack. In [55], Sastry studies the impact of acknowledgement messages on the performance of slotted Aloha using Code Division Multiple Access. This work was done 40 years before the appearance of the IoT networks and considered a totally different context than us.

Presently, with the coming of the IoT networks, the study of the Aloha protocol gained popularity. Zhu et al. [54], provide a mathematical model they consider flexible and capable to adapt to any type of network. The authors use their model to evaluate the performance of two LPWAN technologies, SigFox and LoRaWAN. However, the model is not very clear about the use of acknowledgement messages. The authors mention that messages are repeated multiple times, and they mention the independence of these repetitions. However, the model also considers that some packets are received without any repetition, which implies a kind of feedback between the sender and the receiver. Moreover, the authors of [54] conclude that the repetition of messages is always beneficial and their results show that the higher the number of repetitions, the lower the outage probability. In our work, the number of message repetitions is a parameter. We prove, with analytical and simulation results, that no a general conclusion can be made about the number of repetitions. In several cases, sending with less repetitions is very beneficial.

In this chapter we propose a mathematical modeling of the Aloha No Ack protocol for dedicated IoT networks.

We validate our model with simulation results, and afterwards we explore the model in order to study the impact of some MAC layer parameters on the performance of an IoT cell.

We also compute an optimal Aloha No Ack configuration for several network traffic intensities with the help of our analytical solution. A comparison between this optimal solution and the one operationally used by the SigFox IoT technology provider is included in this chapter.

4.1 Mathematical Model

We present here a mathematical model of Aloha for dedicated IoT networks without considering any acknowledgement. The time is considered unslotted, as it is the case in LPWANs, where the cost of time synchronization can be too important.

We recall that in the case of classical Aloha with acknowledgement messages, a frame retransmission is produced only when the sender node does not receive any acknowledgement before a certain time limit, wich we call *AckTimeOut*.

In the better case, the frame is repeated until the reception of an acknowledgement message confirming the reception of the frame by the receiver node. In the worst case, the sender node does not receive any acknowledgement message from the receiver. Then, the retransmission operation is repeated until the sender node reaches its allowed number of retransmissions. Here, the node drops the packet and the packet transmission is considered failed.

Disabling acknowledgement message mechanism will influence on the retransmission operation.

With Aloha No Ack, the sender node does not wait for any feedback from the receiver node. Then, for each newly created packet, the node transmits a fixed number of frames at the MAC layer. This number of retransmissions, denoted as *K*, is the main MAC parameter we want to study through this model. We use the term of copy and repetition to call the frames retransmissions done for the same packet.

The signification of the variables used in this chapter are summarized in Table 4.1.

Parameter	Parameter description	Range of values
T	Packet generation period	1 ms
T_s	Transmission duration of a frame	$165 \cdot 10^{-6}$ s
π	Probability of a packet generation during T_s	0,0033
K	Number of retransmissions	{1,2,3,4,5}
N	Number of nodes	{10,40,70,100,150,250,500}
G_u	Channel gain of node *u*	
η	Signal to noise ration reception threshold	
N_o	Noise level	
P_{tx}	Transmit power	

Table 4.1: Model parameters and range of values used for numerical results.

4.1.1 Model without the capture effect

We first study the case where no capture is possible at the gateway, meaning that when two frames arrive at the same time at the sink node, both are considered lost. Let *N* be the number of sender nodes in the cell; every node generates a new packet in a period of time denoted *T*. The frame transmission duration is denoted T_s and the probability of a node transmitting a frame within T_s is π.

In the case of Aloha No Ack used in a cell of *N* nodes and without any repetition done at the MAC layer (*K*=1), when a node *u* sends a frame, its success probability is the probability of no other simultaneous transmission from the remaining (*N-1*) nodes during the vulnerability period. When the time is unslotted, the vulnerability period lasts the double of a transmission duration: $2*T_s$. This because potential colliders can start their transmission up to T_s before or after node *u*.

Then, the probability that a node transmits a packet within the vulnerability period is *2*π*, and we deduce that the probability of a node not sending any packet during vulnerability period is: (*1-2*π)*.

Therefore, the probability of no other simultaneous transmission during the vulnerability period, or equivalently the probability of a successful transmission for node *u* is:

$$P_s(K = 1, u) = (1 - 2\pi)^{(N-1)}$$

In the case where we transmit more than one copy of the packet at the MAC layer level, *i.e.* K>1, when a node *u* sends a packet, its success probability is that at least one copy among the *K* transmitted is successful. This is similar to saying that no other user is sending during the vulnerability period corresponding to at least one of the *K* copies.

Following the same logic as above, the probability of a node sending one if its K frames during a vulnerability period is: *2*π*K*. This is equivalent to increasing the traffic intensity of a node K times.

Then, the probability of a node not sending any frame during the vulnerability period of a node *u* is: (*1-2 π*K*).

Therefore, the probability of no transmission occurring from the (*N-1*) competing nodes during the vulnerability period of node *u* is: $(1-2\pi \cdot K)^{(N-1)}$.

Finally, the probability of at least one concurrent transmission from another node during each of the *K* copies is:

$$P_{col} = (1 - (1 - 2\pi \cdot K)^{(N-1)})^K$$

Hence, the probability of success when *K* copies are sent at the MAC layer, *i.e.* the probability of no other user sending during at least one of the *K* vulnerability periods of node *u* can be expressed by:

$$P_s(K, u) = 1 - \ (1 - (1 - 2\pi \cdot K)^{(N-1)})^K$$

4.1.2 Model with simple capture effect

In previous equations, when two frames arrive at the same time at the receiver node, we consider that both of them are lost, while in many cases the receiver could be able to extract the most powerful signal, a phenomenon known as the capture effect.

The enhancements obtained by taking advantage of the capture effect have already been proven in the literature since decades.

Goodman et al [38] proved through a mathematical model that the capture effect is good for overall network performance in the case of a slotted Aloha and this is beneficial even for nodes with the lowest power level. In [42], Sylvie et al. investigated the phenomenon by modeling the channel backlog as a Markov chain and they proved that the capture effect of what they call multipacket reception can stabilize the slotted Aloha throughput with infinite user condition.

Some recent works also studied the impact of capture. Slahttin et al. [43] propose a mathematical way to calculate the throughput of an Aloha network, with and without including capture at the reception; they validate their model with experimental results obtained by developing an IoT network with tinyOs sensor nodes. However, in their work, they do not mention at all the acknowledgement messages, so we ignore if they are present or not. They also do not give any information about the retransmission mechanism, not even regarding the number of allowed retransmissions. The authors use the throughput as a metric and they change only the packet size and the generated traffic intensity.

Dmitry et al. [44] also provide a mathematical model, but only for LoRaWAN networks with class A devices. In their model, they take into account the capture effect, the propagation losses, the retransmissions and even the two types of acknowledgement messages used by this class of the LoRaWAN standard. A validation by NS3 simulations is presented in their paper by using previously developed simulation models [45-46]. This contribution stays a technology limited study, while we aim to provide a technology independent model.

Therefore, we present in the following how we include the capture effect to our previously presented model, without adding a lot of extra-complexity to it, such as when considering specific technology parameters.

We consider that, if two frames arrive at the same time, the gateway might possibly extract one of them so we do not necessarily consider them as both lost. For the sake of simplification, we assume that, if more than two transmissions arrive simultaneously at the receiver node, no capture is possible.

We assume that we know the distribution of the channel gain over all the nodes. Given that a node u transmits a frame in a period of time T_s and its channel gain to the gateway G_u, if there is a single other transmission from a node v, the frame from u will be decoded with probability: $P[G_u<A_u]$, where $A_u = (G_u/\eta) - (N_o/P_{tx})$. Since all the parameters are known.

Given the channel gain distribution, we can easily compute $P[G_u<A_u]$.
Then, for the case of a single transmission at the MAC layer, *i.e.* $K=1$, when a node u sends a frame, it is successfully received if one of two conditions is met. The first one is that no other simultaneous transmission is happening from the ($N-1$) other nodes, which we already expressed by the definition of $P_s(K = 1, u)$ above.

The second condition is that, there is only one simultaneous transmission from a certain node v and no other transmission from the ($N-2$) other nodes, which can be expressed by:

$$P_{sim}(K = 1) = (N - 1) \cdot 2\pi \cdot (1 - 2\pi)^{(N-2)}$$

The frame from node u will be well decoded by the receiver gateway with probability $P[G_u<A_u]$. The second condition would be mathematically presented as:

$$P_{cap} = (N - 1) \cdot 2\pi \cdot (1 - 2\pi)^{(N-2)} \cdot P[G_u < A_u]$$

Hence, by joining the two conditions, we obtain the probability of a frame successful transmission under capture effect:

$$P_{cs}(K = 1, u) = (1 - 2\pi)^{(N-1)} + (N - 1) \cdot 2\pi \cdot (1 - 2\pi)^{(N-2)} \cdot P[G_u < A_u]$$

For the case of more than one frame transmitted at the MAC layer, *i.e. K>1*, we seek for the probability of at least one frame among the K copies sent by node u being received by the gateway. To do so, we start by expressing the probability of two main events. The first one is the probability of no other simultaneous transmission being done by the remaining (*N-1*) nodes during at least one vulnerability period among the K transmissions of node u, we already expressed above as $(1\text{-}2\pi\cdot K)^{(N-1)}$.

The second probability is the one of a single simultaneous transmission from a certain node v and no other simultaneous transmission from the other (*N-2*) nodes. Then, we know that the frame of node u will be decoded with the probability $P[G_u<A_u]$, we express this condition by:

$$P_{sim}(K) = (N-1)\cdot 2\pi\cdot K\cdot(1-2\pi\cdot K)^{(N-2)}\cdot P[G_u < A_u]$$

Then, by combining the probabilities of these two events, we can compute the probability of failing K successive times for node u, which would imply the loss of a packet under Aloha No Ack with *K* retransmissions:

$$P_{col}(K) = [1-(1-2\pi\cdot K)^{(N-1)} - (N-1)\cdot 2\pi\cdot K\cdot(1-2\pi\cdot K)^{(N-2)}\cdot P[G_u < A_u]]^K$$

Hence, the packet success probability in Aloha No Ack with *K* retransmissions when accounting for the capture effect is given as:

$$P_{cs}(K>1,u) = 1-[1-(1-2\pi\cdot K)^{(N-1)} - (N-1)\cdot 2\pi\cdot K\cdot(1-2\pi\cdot K)^{(N-2)}\cdot P[G_u < A_u]]^K$$

4.2 Model validation through simulation

4.2.1 Simulation Setup

In our simulation study, we use the WiFi model of ns3.26. We note that the capture effect was not modeled in ns3.26 and it has only been implemented in later versions of the simulator, after our study.

To simulate Aloha No Ack, we disabled the acknowledgement message generation at the sink node. At the sender nodes side, we do not wait for any acknowledgement in the case of $K = 1$. For $K > 1$, we use the *AckTimeOut* duration to trigger the following frame transmission. More precisely, the time between two consecutive copies corresponding to the same packet is the *AckTimeOut* duration. We decide to model this duration by a random variable, taking a value from zero to $\frac{T}{K}$ seconds. The sender node waits for this period, as if to detect a lost frame before starting the next frame transmission. The use of this random retransmission parameter is both realistic and in line with the frame transmission independence property considered in the analytical model. The other simulation details are in line with the description given in Chapter 3.

We simulated the Aloha No Ack protocol for different network densities and we changed the value of the number of retransmissions *K*. The ranges of values tested for the different MAC layer parameters are given in Table 4.1. The probability of a packet generation during a period T_s, i.e. π, is obtained by the expression: $\pi=T_s/T$. Considering the number of nodes used in our simulation, the range of values for the network load, computed as $\pi \cdot N$, is: 0.033, 0.132, 0.231, 0.33, 0.495, 0.825, 1.65 and 3.3.

4.2.2 Simulation and numerical results

We here compare the simulation results with the analytical model results for the case without capture effect.

As we can see below in Figure 4.1, Figure 4.2 and Figure 4.3, the simulation results and the mathematical model results are very similar. We can say that these results validate our mathematical model and the Aloha No Ack network behavior with respect to the variation of the number of retransmissions parameter. The results are in line with those already presented in Chapter 3, showing the important drop in packet success probability as the number of nodes increases.

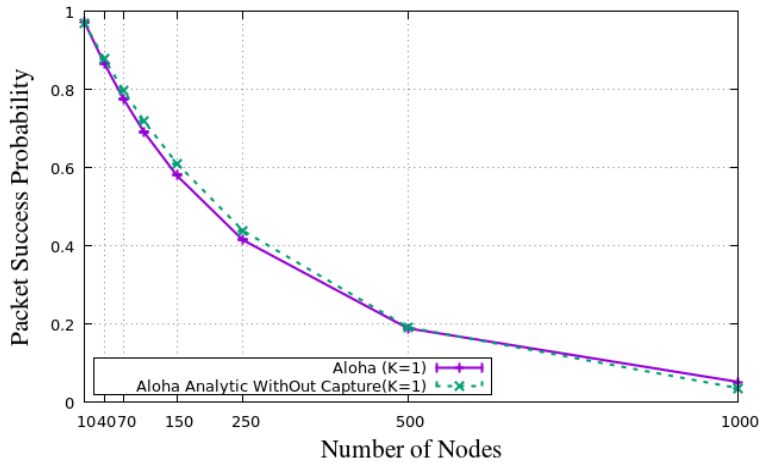


Figure 4.1 : Analytical model and simulation results when K=1

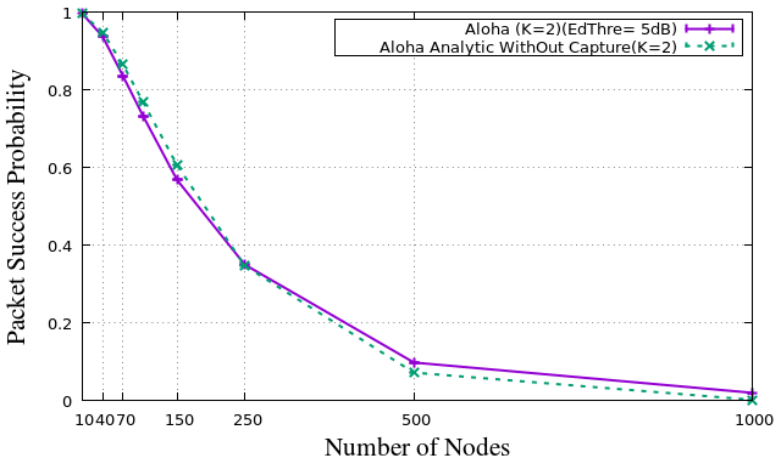


Figure 4.2 : Analytical model and simulation results when K=2

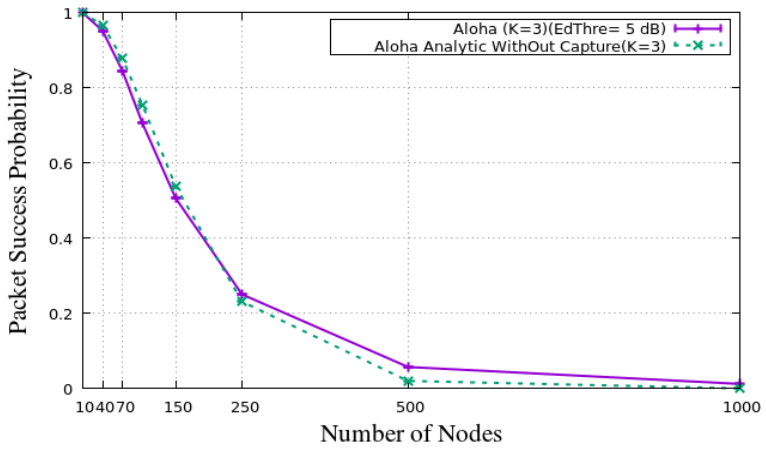


Figure 4.3 : Analytical model and simulation results when K=3

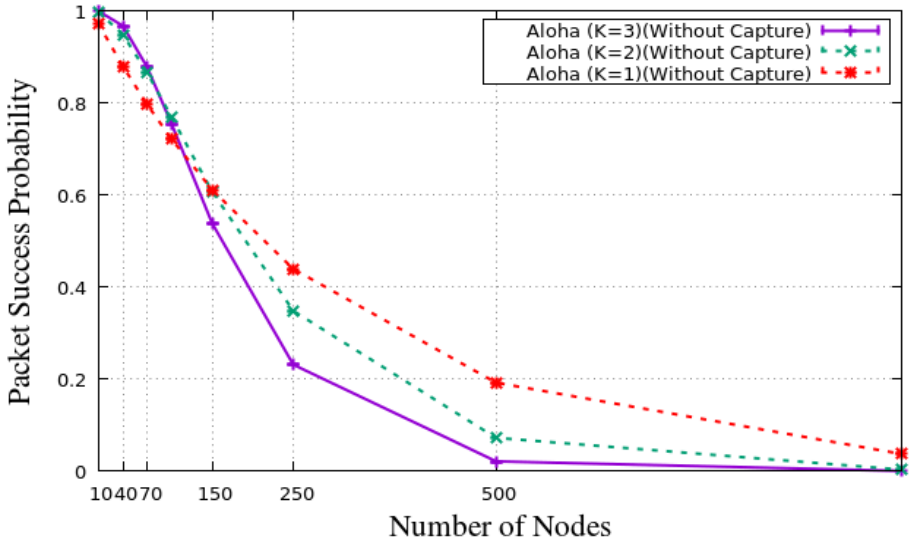


Figure 4.4 : Analytical model results for different K values.

We note that the proposed analytical model can predict the packet success probability of an IoT cell when knowing the node density, traffic intensity and the allowed number of retransmissions.

In Figure 4.4 we use the analytical model to compare the results obtained for different values of *K*. Interestingly, we notice that there is no general optimal value for the number of retransmissions and that, when the load increases, the reduced load obtained with $K = 1$ outperforms the other configurations.

4.3 Numerical results with capture effect

In the following, we explore our analytical model to evaluate the impact of some important parameters on the IoT network performance. In this section, we study the impact on the PSP of the capture effect at the sink node level.

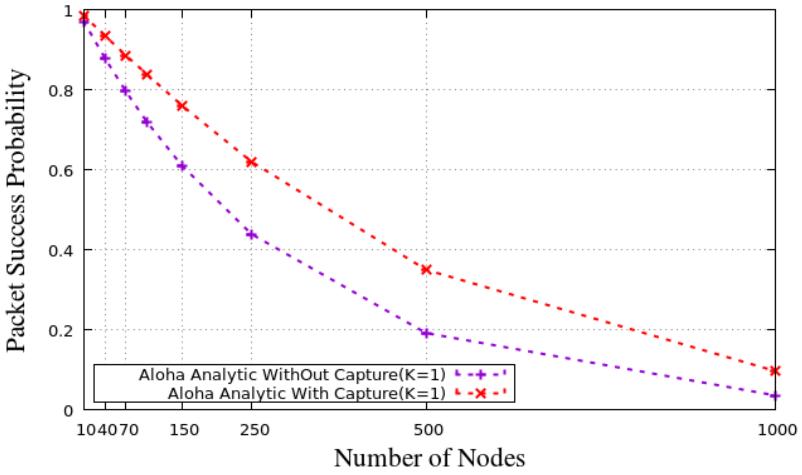


Figure 4.5 : Packet success probability with and without capture effect when K=1

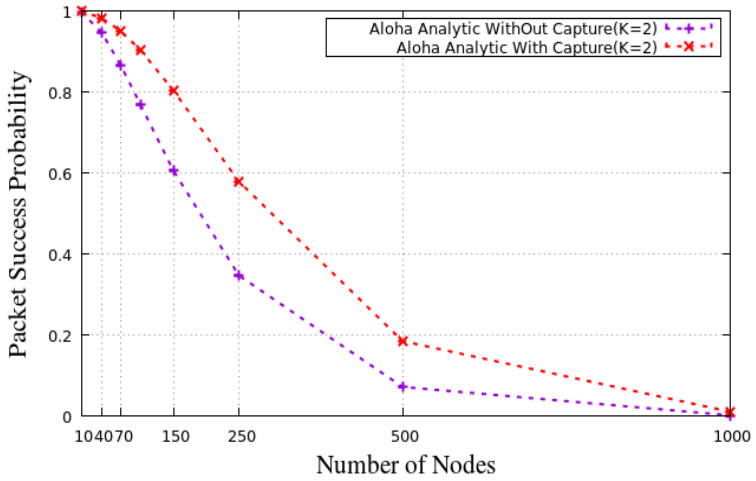


Figure 4.6 : Packet success probability with and without capture effect when K=2

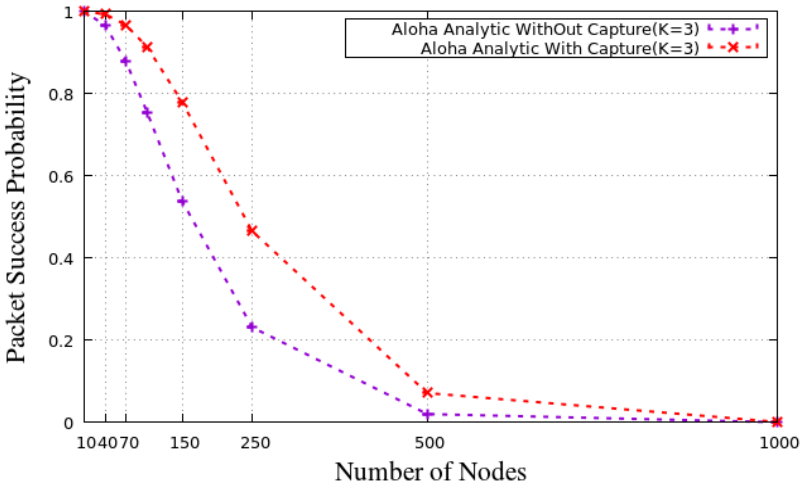


Figure 4.7 : Packet success probability with and without capture effect when K=3

We can see in Figure 4.5, Figure 4.6 and Figure 4.7 that the capture effect enhances the general IoT network performance in terms of PSP. In the case of K =1, in Figure 4.5, the capture effect is always boosting the performance, especially for N = 250 and N = 500, where the PSP gain reaches 20%. For K = 2 and K = 3, the capture effect is also very beneficial, especially for N = 250, where the PSP improves by more than 20%. This amelioration starts to get smaller from N = 500 and almost disappears for N = 1000, which is due to an increased channel congestion where the capture effect becomes less efficient.

It is notable that the capture effect cannot cope on its own with the high channel load of dense IoT networks.

4.4 Radio propagation error model

The results obtained above consider that the unique reason for packet loss is represented by the collisions happening on the radio channel. However, the radio propagation errors represent the main challenge that the wireless network have known. Plenty of physical phenomena could cause radio propagation errors, such as path loss, fading, shadowing, additive white Gaussian noise and interference from other technologies.

Several studies have been conducted in order to study these phenomena. Hata [49] introduced an empirical propagation loss formula based on real experimental reports for land mobile radio services. Then, other research works tended to use a computer-based propagation prediction model for outdoor networks [50-51].

IoT network are also wireless networks, hence they are concerned by the radio propagation errors. Recent contributions have been conducted to evaluate the impact of radio propagation errors on the IoT network performance and propose prediction models. Salaheddin *et al.* [52] provided a hybrid prediction model for the radio channel, that combines neural networks and the COST 231 empirical model proposed by Hata [49] for a better accuracy. The authors validated their model with practical results obtained in a LoRaWAN network. El Chall *et al.* [90] present a propagation loss model for LoRaWAN networks and they prove the accuracy of the model by extensive measurements done with LoRaWAN nodes implemented in urban and rural areas in Lebanon.

All these studies show that the long distance links used in LPWANs are error prone. As a matter of fact, the reason behind the frame retransmission mechanism used in Sigfox is that they account for a radio propagation error. Therefore, we refine our previously presented model to consider the probability of a propagation error. We do not integrate a complex radio propagation model; instead, we simply denote the radio propagation success probability for a frame as P_p. We study different values of P_p in order to evaluate its impact.

4.4.1 Analytical model without capture effect

After introducing the parameter P_p the probability that user u transmitting a frame is successful in a given T_s when using Aloha No Ack is:

$$P_{sp}(K = 1, u) = P_p \cdot (1 - 2\pi)^{(N-1)}$$

When K retransmissions are used, the probability for a user u transmitting a packet to be successful is:

$$P_{sp}(K, u) = 1 - \ (1 - P_p \cdot (1 - 2\pi \cdot K)^{(N-1)})^K$$

4.4.2 Analytical model with simple capture effect

When using a capture effect model, after introducing the P_p parameter, the probability that user u transmits a successful frame in a given T_s when using the Aloha No Ack protocol is:

$$P_{cp}(K = 1, u) = P_p \cdot (1 - 2\pi)^{(N-1)} + (N - 1) \cdot 2\pi \cdot (1 - 2\pi)^{(N-2)} \cdot P[G_u < A_u]$$

We note that, for the second term in the equation above, the quality of the radio channel is already considered in the capture effect model.

When K retransmissions are used, the probability for a user u transmitting a successful packet is $P_{cp}(K, u)$:

$$P_{cs}(K, u) = 1 - [1 - P_p \cdot (1 - 2\pi \cdot K)^{(N-1)} - (N - 1) \cdot 2\pi \cdot K \cdot (1 - 2\pi \cdot K)^{(N-2)} \cdot P[G_u < A_u]]^K$$

Since this is more realistic, for the rest of this chapter, we show only the results for the model with capture effect. With the help of our model, we plot the performance of the IoT network in terms of PSP for different P_p values (0.5, 0.8 and 1), with the same previous range of values for the number of retransmissions. These results are shown in Figure 4.8, Figure 4.9 and Figure 4.10, for K = 1, 2 and 3, respectively.

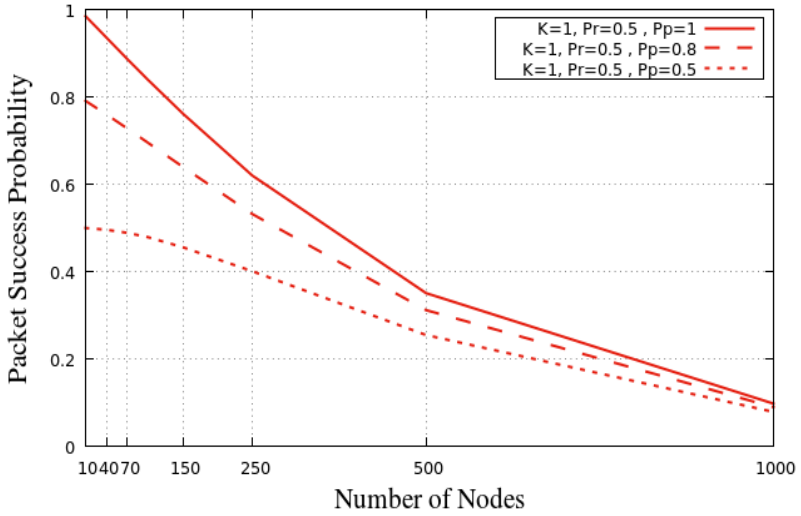


Figure 4.8 : The impact of radio propagation errors when K=1.

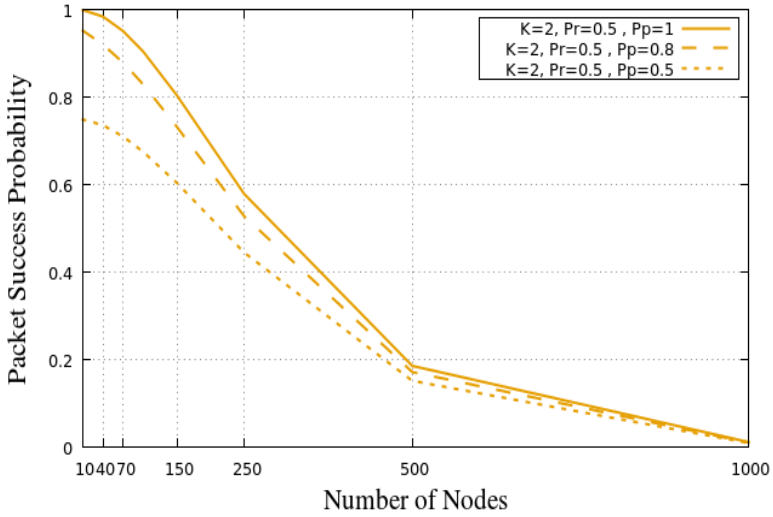


Figure 4.9 : The impact of radio propagation errors when K=2.

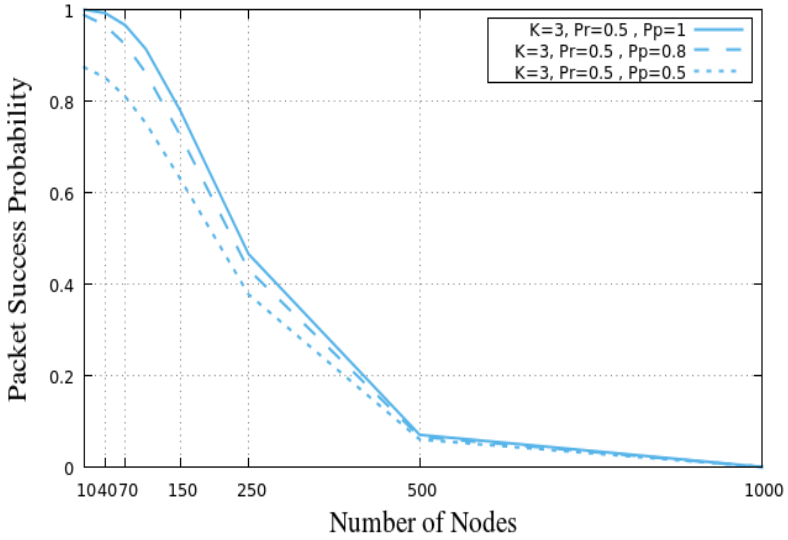


Figure 4.10 : The impact of radio propagation errors when K=3.

In these figures, we notice that the propagation success probability is having more impact on the lower K values. For K = 1, in Figure 4.8, the value of P_p is impacting significantly the PSP results: for small N values, we can reach a difference of 20 % between P_p = 0.8 and P_p = 1, and a difference of 50% between P_p = 0.5 and P_p = 1. Meanwhile, for N = 1000, where the density is already high, the network performance is already poor, even without introducing a radio propagation error.

For K = 2, shown in Figure 4.9, the impact of the P_p parameter exists as well, but it is less important than the previous case. For small N, the biggest difference between P_p = 0.5 and P_p = 1 reaches 22% (instead of 50% for K = 1) and, starting from N = 500, the impact becomes insignificant.

For K = 3, shown in Figure 4.10, the P_p impact is even much smaller than for the two previous cases: the maximum difference between P_p = 0.5 and P_p = 1 is 17% for smaller N, and starting from N = 250 the gap becomes negligible between all P_p values. The presence of radio propagation errors is the reason why a technology like SigFox tends to use a value of K = 3, which makes the network more immune face to channel problems, especially for low dense networks.

4.5 Optimal retransmission number

Dedicated IoT networks are designed to handle a large number of devices sending data to a same sink node in one hop configuration. There could be thousands of devices connected to a same gateway in single cell [47-48], as shown by some recent works studying the performance of IoT networks in high dense conditions. In [47], Orestis *et al.* propose, through stochastic geometry tools, a way to improve the LoRa network performance in case of high interference level caused by a large number of nodes. In [48] Mariusz *et al.* propose as well an enhancement of the LoRa network performance for dense scenarios while exploiting a built-in adaptive data rate mechanism. However, the mechanism widely used in current deployments is a statically configured number of retransmissions, such as the 3 retransmissions used by Sigfox.

In this section, we exploit our model to investigate the optimal value of the retransmission number while taking into account the radio propagation error (or, more precisely, the frame success probability P_p). We here include more values of K (up to 5), in order to generalize a bit more our study, and we keep the same range of values as in the previous section for P_p.

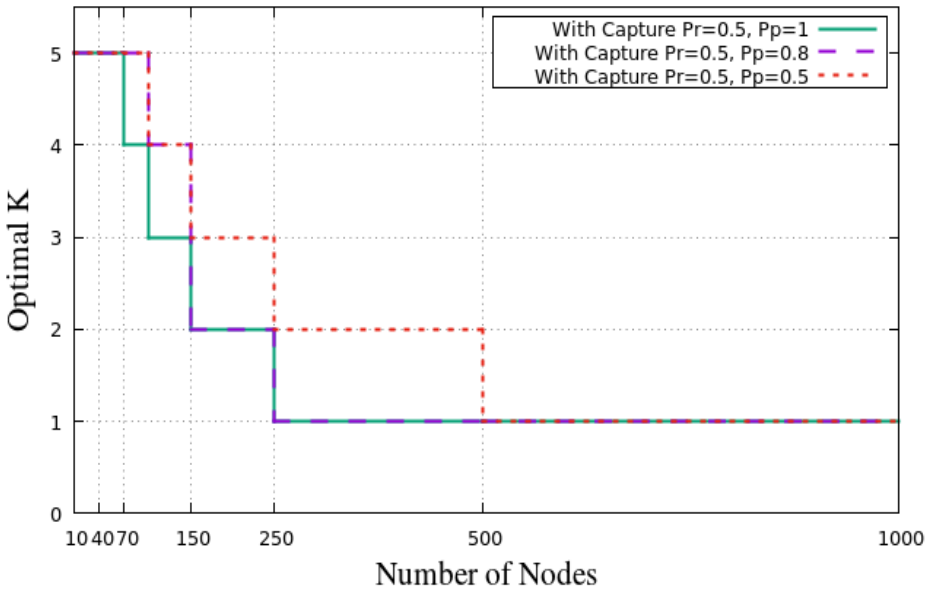


Figure 4.11 : Optimal value of K as a function of the number of nodes.

In Figure 4.11, we show the optimal value for K with a varying number of nodes. We notice that the optimal K value depends on the network density: for low dense networks, the optimal K tends to have larger values, while for high dense networks the optimal K tends to be smaller. The fact that the optimal K value decreases with the increase of the network density is true for all values of P_p. However, the P_p parameter is having an impact on the results, which are shifted for different P_p, although they show the same decreasing behavior when the density increase.

These results confirm our previous observations that $K = 3$ is not the best solution all the time, even when taking into account the radio propagation error. However, we have to be aware that this conclusion is based only on PSP results and in order to have a fair judgment we need to take into account other metrics as well, such as the energy consumption or the node activity time. Our analytical model does not measure any energy-related metric, but we believe that, for the case of a MAC solution not using ACK messages and where the number of retransmissions is constant, the node activity time is very linked to the value of K and we can simply say that, when K is bigger, the general activity time of the network is bigger and vice versa. We will validate this theory through simulation in Chapter 5.

Hence, we can say that $K = 3$ could be the best choice for low dense networks, since it assures the compromise between PSP and activity time compared to other values of K. Meanwhile, for high dense networks, $K = 3$ is far from being the best choice, since we can get better PSP results, as shown in Figure 4.11, while also ensuring less activity time periods with lower K.

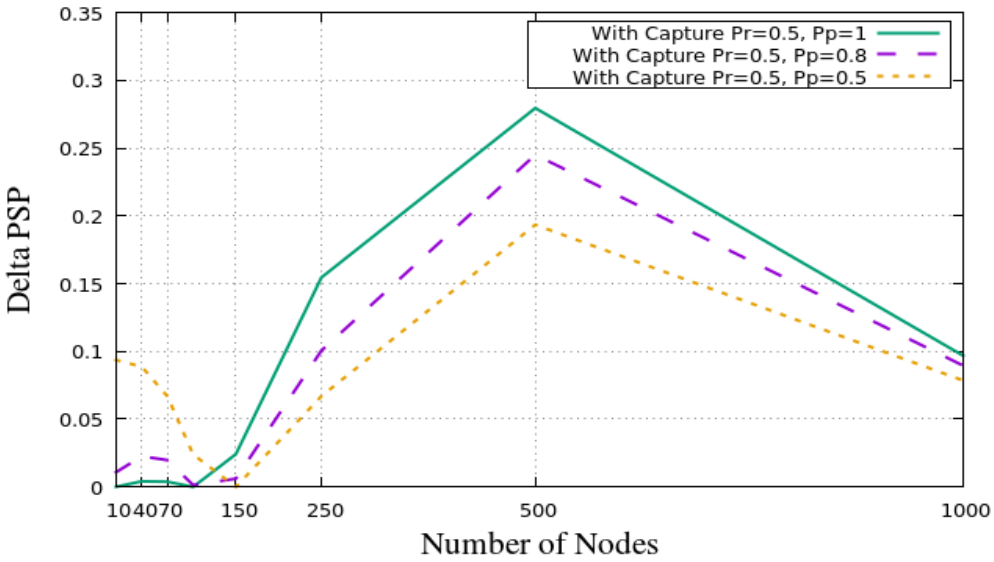


Figure 4.12 : Difference in terms of PSP between the optimal K and K = 3.

To better understand these results, we show in Figure 4.12 the difference in terms of PSP between a network using the optimal K value and one using a fixed $K = 3$. Figure 4.6 we show the difference between the PSP obtained by the optimal retransmission number and the PSP obtained by a retransmission number of 3.Practically, this can be considered as the loss recorder by a solution such as Sigfox with respect to the optimal value, for different propagation error probabilities. As we can see, the difference with respect to the optimum in terms of PSP can reach more than 25% for certain configurations.

4.6 Impact of the number of channels

The use of multiple channels is used in all kind of wireless networks in order to enhance the network performance. For example, in [56] the authors studied analytically the impact of the number of channels and interfaces on the wireless network performance. They showed that, for an arbitrary network, the multi-channel could cause a network capacity loss if the number of interfaces of a node is less than the number of available channels. Meanwhile, for a random network, a single interface per node is sufficient to take advantage of the multi-channel.

In [54], Zhu *et al.* analyze jointly interferences in the time-frequency domain using a stochastic geometry model. They use the card tossing model to represent how collisions are produced in the two dimensional (2D) time-frequency domain. The authors apply their model on LPWAN technologies, SigFox and LoRaWAN. The authors present the outage and throughput results for only the multi-channel case and they do not mention the impact of the use of multiple frequencies.

While multi-channel is heavily used in dedicated IoT networks, in this thesis we did not include the multi-channel capacity in our simulations and in analytical model. Instead, we aim to make the single channel sharing more efficient, without any change at the physical layer or at any other upper layer. As we will show in the following chapters, we believe that we are able to reach our goal by tuning the different MAC layer parameters.

The use of a single channel makes the performance evaluation study easier to perform, for sure, but the major IoT technologies, SigFox and LoRaWAN, both use multi-channel. In this section, we test whether our results can be easily extended to multi-channel operation.

For this, we use our analytical model to find a link between the packet success probability when a single channel is used and the packet successful probability when multiple channels are used. To do so, we generalize the case by considering two scenarios with different number of available channels, C and S. We suppose that S is nothing but a multiple of C and x is the factor of multiplication.

Then, we try to find the relation between the two success probabilities, when *C* and when *S* channels are used, respectively. We only conduct this analysis for a model without capture effect.

Using the model described in Section 4.1.1, the packet success probability for a node *u*, with *N* other competitors on the channel and using *K* retransmissions can be generalized to a scenario with *C* channels, as follows:

$$P_s(C,K,N,u) = 1 - \ (1-(1-2K/C \cdot T)^N)^K$$

Our strategy is to take this scenario with *C* channels as reference, and to compare it with a scenario with $S = x \cdot C$ channels. We want to find the number of nodes *M* that result in the same success probability for the scenario with *S* channels, as the *N* nodes in the scenario with *N* channels. Formally, this can be written as:

$$P_s(C,K,N,u) = P_s(S,K,M,u)$$
$$1 - \ (1-(1-2K/C \cdot T)^N)^K = 1 - \ (1-(1-2K/x \cdot C \cdot T)^M)^K$$

After a few simplifications and applying a logarithmic function on both sides of the equality, we obtain:

$$N \cdot ln(1-\frac{2K}{C \cdot T}) = M \cdot ln(1-\frac{2K}{x \cdot C \cdot T})$$

We are now ready to answer the following question: how much increases the capacity of a dedicated IoT network when the number of orthogonal channels it uses is multiplied by *x*?

$$\frac{M}{N} = \frac{ln\left(1-\frac{2K}{C \cdot T}\right)}{ln\left(1-\frac{2K}{x \cdot C \cdot T}\right)}$$

Interestingly, at first sight this is not a linear function, as it might be expected. However, we plot this function in Figure 4.13 for a scenario where $S << T$, meaning that the number of channels is much lower than the number of possible transmissions in a transmission period. We notice that, when this assumption is respected, the capacity of a dedicated IoT network, in terms of number of nodes, increases linearly with the number of channels.

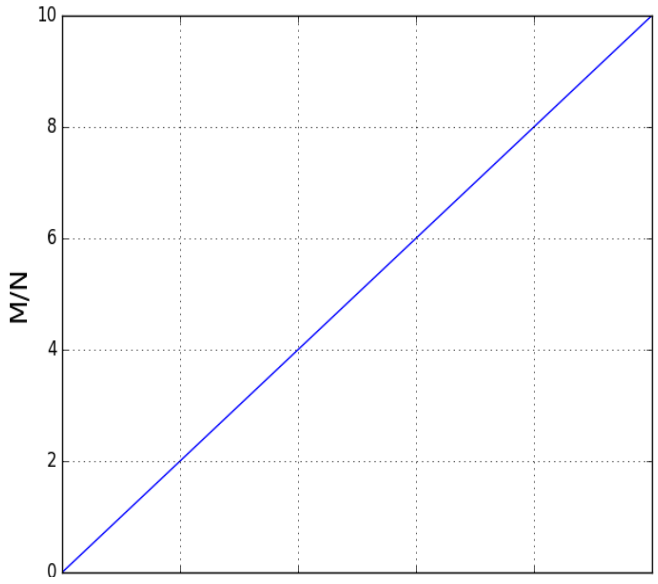


Figure 4.13 : Capacity increase in multi-channel scenarios.

We believe that these results confirm our assumptions that the use of multi-channels will not change the behavior of the network. Multi-channels might make the network more immune to the node density, so the drop of PSP performance will in general happen for a larger network density when we use more channels. However, we are reassured that the figures we obtained for a single channel will not change shape, but the phenomena we observe throughout this thesis would just be observed at higher network densities.

5. A Detailed Study of CSMA without Acknowledgement Messages

The Carrier Sense Multiple Access (CSMA) is one of the main medium access control solutions. CSMA is mainly used by the IEEE 802.11 standards for wireless local area networks [57] [68]. In wireless networks, the stations are not able to detect collisions while transmitting. Therefore, the CSMA variant used in such a context is CSMA with Collision Avoidance (CSMA/CA).

The CSMA/CA protocol has a mechanism to avoid the collisions by sensing the channel if idle before transmissions and by acknowledgement messages [57] [68]. An optional prior negotiation can be done through the exchange of the control packets Ready To Send (RTS) and Clear To Send (CTS) between the sender and the receiver [57] [68]. In our work, we do not consider the phase of negotiation, so the RTS and CTS messages exchange is disabled.

Several works have been conducted to study the CSMA/CA protocol [58] and even to propose enhancements [59]. In [58], Bianchi proposes an analytical model to compute the CSMA/CA throughput for a finite number of terminals and for ideal channel conditions. Lacage et al. [59], propose an adaptive rate algorithm for the IEEE 802.11 protocol and show the improvement obtained by their contribution through experimentations.

Since the appearance of IoT networks, the Aloha MAC protocol was somehow privileged in this context, because it allows for much simpler IoT nodes. However, for indoor IoT networks, the WiFi Alliance developed a CSMA-based MAC layer solution, denoted WiFi-HaLow or IEEE 802.11ah [WiFi-HaLow standard doc]. Meanwhile, some research works tend to test the performance of the CSMA/CA MAC protocol for outdoor IoT networks [60-63].

Pham [60] added a carrier sense mechanism to devices of a LoRa network, by exploiting the Channel Activity Detection (CAD) procedure of the LoRa devices. The author shows how the CSMA protocol renders the LoRa network more robust towards collisions. Using a simulation approach, To and Duda [63] demonstrate similar properties. Moreover, they show that using a non-persistent CSMA approach results in an energy consumption close to the one obtained by Aloha.

Nikos et al. [61], use a persistent CSMA (p-CSMA) MAC solution in a LoRa network and evaluate it with the help of the NS3 simulator [67]. The authors show how the p-CSMA decreases the number of collisions, it enhances the hidden devices detection and it improves the packet reception ratio. However, the paper does not include any energy consumption results.

Zucchetto and Andrea [62], test three MAC protocols: Aloha, HYB and CSMA in a dedicated IoT network. The HYB is a hybrid access scheme where the node is divided into slots, these slots are divided into two groups and each group uses a different access scheme [62]. They consider a scenario of high density and long-range network. The paper results show the superiority of the CSMA MAC solution in terms of success probability. They also present CSMA as the best energy-efficient protocol. However, Zucchetto and Andrea [62], only consider the case where a single frame is sent by the MAC layer. The acknowledgement and the frame retransmission are not considered for simplification purposes.

A key parameter of the CSMA protocol is the Clear Channel Assessment (CCA) threshold. The CCA threshold takes the values of a power level. When a node senses the channel, if the sensed signal power is below the CCA threshold, then the node considers the channel as free and transmits its frame. Otherwise, the node considers the channel as busy and keeps sensing the channel until free, before sending [56][68].

All the aforementioned contributions in the context of IoT networks did not mention the CCA threshold parameter in their studies. Hence, the authors considered that, when the CSMA protocol is implemented, every node in the cell is able to hear all its contenting nodes. Unfortunately, this assumption is far from being real for dedicated IoT network, since in such network the cell size can reach 15 km in rural areas and 5 km in urban areas [62].

While for other types of wireless networks, the CCA threshold has been studied in order to measure its impact on the network performance or to use it to enhance the network performance.

Yuan et al. [64], propose an adaptive CCA approach that improves the IEEE 802.15.4 network performance when a heavy interference is present. The authors treat a specific case when an IEEE 802.15.4 network is impacted by IEEE 802.11b/g nodes interference. Yuan et al. [8] show, using OPNET simulations, how they improve IEEE 802.15.4 network throughput with adaptive CCA, especially when high IEEE 802.11b/g nodes interference is present. However, the proposed solution does not reduce the number of collisions, it only reduces the inhibition loss. This latter loss happens when a packet is discarded by a node due to channel access failure.

Charalampos et al. [65], propose a machine-learning based solution to enhance the CCA mechanism of IEEE 802.15.4 protocol. Authors show how their proposed CCA mechanism helps the IEEE 802.15.4 nodes to detect LoRa interference and increases by 30% the overall accuracy of the CCA decision.

Maite et al. [66], uses a real-world deployment of wireless sensor network (WSN) in order to take advantage of the CCA threshold to improve the performance and the topology of the network. The authors propose a cross-layer approach by evaluating the impact of the CCA threshold on the routing protocol used in their multi-hop WSN. The implementation results show how lower CCA threshold values improve the packet data ratio of the network and reduces the path cost, especially for farther nodes (2 hops and more from the sink). The results show as well that the change of the CCA threshold does not impact the energy consumption. However, the work was limited to internal interference since the deployment was in the countryside, with the absence of any kind of external interference.

In this chapter, we investigate the use of a CSMA No Ack-based MAC protocol for dedicated IoT networks. The novelty of our contribution, with the respect to the aforementioned works, is the study of the CSMA No Ack protocol in a dedicated IoT context, while including the CCA threshold parameter. The CCA threshold represents the device sensitivity, which reflects directly the capacity of the node to sense other simultaneous transmissions. The devices that are used in a dedicated IoT context are low cost devices, hence, a node would never be able to detect all its contenting nodes. Therefore, we introduce the CCA conflict ratio, which represents the portion of the contending nodes that an IoT device can sense. With the help of these two CCA indicators, we investigate the feasibility of a CSMA No Ack-based MAC protocol for IoT networks.

To the best of our knowledge, this is the first contribution that includes the CCA threshold analysis in a CSMA MAC solution for dedicated IoT networks. And this is also the first work that introduces the CCA conflict ratio of the nodes.

In Section 5.2, we present our simulation methodology. In Section 5.3, we study the performance of CSMA with acknowledgement messages. In Section 5.4, we study CSMA without acknowledgement messages, denoted as CSMA No Ack.

5.1 Simulation Methodology

We briefly presented our simulation approach in Chapter 3, but without entering in too many details. In this section, we summarize the modifications we brought to the ns3 simulator [11], which we use to study a dedicated IoT network with N sender nodes and one sink node. The most important simulation parameters are provided in Table 5.1. While we provide these values for reproducibility purposes, we argue that our study is agnostic to the physical layer parameters and models. We acknowledge that, because of this choice, our findings do not directly apply to a specific IoT technology. Indeed, our intention is to be as generic as possible and study a dedicated IoT network based on its particular topology and traffic model, not on the specific functions it implements at the physical layer.

Parameter	Value
Number of retransmission	{1,2,3}
RTS/CTS messages	Disabled
Frequency	5.180 GHz
Transmission power	16 dBm
Propagation loss model	Log Distance
Propagation delay model	Constant Speed Mode
Transmission data rate	6 Mbps
Transmission opportunity	$165 \cdot 10^{-6}$ s

Table 5.1 : Simulation MAC layer parameters.

Basically, as in Chapter 3, we set our simulation in order to obtain a network topology consisting of a single cell of radius r, with a base station sink node situated in its center. The IoT nodes are uniformly distributed inside this area and they all share the same channel. For the CSMA No Ack model, we used the ns3 AdhocWifiMac at the MAC layer, using the parameters indicated in Table 5.1. The CCA threshold is set by default at -99 dBm. However, as explained below, we studied different values for this parameter in our work.

Another parameter that we observe in detail is the number of retransmissions used by the CSMA No Ack protocol. Indeed, if the reception of a message is not confirmed by an acknowledgment message, the CSMA/CA MAC layer retransmits the message in question. In the case of CSMA No Ack, there will never be ACK messages and the normal behavior of the sender node in ns3 in this case is to retransmit a copy of the frame. We exploit this property in the case the number of retransmission is higher than 1. More precisely, we use the acknowledgement timeout as the trigger of the next copy transmission, as explained below. This allows us to implement frame repetition by relying on existing mechanisms.

Removing the acknowledgement messages is a little bit tricky to do while keeping the AdhocWiFiMac model functioning correctly. We first block the creation of any ACK message at the sink node level. We do it by modifying the function MacLow::ReceiveOk()of the file mac-low.cc in the WiFi model (see annex). For the sender node, side we use the acktimeout as trigger and this is done by making the function MacLow::GetAckTimeout()of the same file return a random value, in order to avoid repeated collisions between nodes due to transmission synchronization. We take care also of the last copy transmission, or the frame where we reach the maximum transmission number. In this case, the node must not wait for any acktimeout duration and it has to go right back to sleep after sending the copy. To handle this we modify the function MacLow::StartTransmission() of the same file and we call the disableAck() function for the last frame transmission. In this case, we still need to update the MAC layer parameters, like the retransmission number and the backoff window size, which is not done automatically once disableAck() is called. We do this in the dca-txop.cc file of the AdhocWiFiMac model, and more precisely in the DcaTxop::EndTxNoAck() function, where we now call the WifiRemoteStationManager::ReportFinalDataFailed() function of the file wifi-remote-stationmanager.cc. Finally, we change the CCA threshold in the main simulation file by calling the physical layer function SetCcaMode1Threshold() through a pointer to the wifi-phy model.

5.2 CCA conflict rate

The results in Chapter 3, as well as most of the results in the literature, consider that the nodes have a large carrier sense range, covering all of their contenders for channel access. As explained, this assumption is particularly unrealistic in a dedicated IoT scenario, where the nodes have much cheaper and simpler electronics compared to an IoT base station, resulting in a reduced receiver sensitivity. We therefore argue that it is not realistic to consider that a node senses all the other nodes in the cell. By changing the CCA threshold of the nodes, we can model this phenomenon, where only a part of the transmissions towards the base station can be sensed by the nodes. Indeed, depending on their position in the network and on their CCA threshold, nodes can have a certain number of hidden interferers, a phenomenon well known in the literature [16].

To assess the impact of the hidden terminals in our network, we define a metric denoted as the CCA conflict rate. This metric is calculated for each node and it shows the ratio of nodes in the cell with which the considered node is in contention, in other words the rate of nodes in the cell that are in the CCA detection zone of the considered node. This parameter depends directly on the value of the CCA threshold and it is calculated for a node *A* as follow:

$$CCA_{CR_A} = \frac{1}{N-1}\sum_{i \in N} \frac{R_{x_i^A}}{T_{x_i}}$$

where $R_{x_i^A}$ represents the number of frames overheard by node *A* from the total T_{x_i} frames transmitted by node *i*. Our goal is to measure the number of neighbors of node *A*, while also accounting for the probabilistic nature of the radio propagation model.

Indeed, in some cases, only a part of the messages transmitted by node *i* actually activate the carrier sense mechanism of node *A*, and this definition allows accounting for these situations. In this chapter, we study the CCA conflict rate of each node and verify whether this metric is linked to the node packet success probability and energy consumption. For this, in our simulations, we calculate the CCA conflict rate of each node for different CCA thresholds and network densities.

5.3 Impact of Clear Channel Assessment threshold

In this section, we study the effect of the CCA threshold on a network using the CSMA No ACK protocol at the MAC layer level in an IoT context, by evaluating the PSP and the time spent by the nodes in an active state. We have previously presented this protocol in Chapter 3. Meanwhile, in this chapter, we investigate a more realistic implementation of CSMA No Ack for LPWANs, by studying different receiver sensitivity levels for the IoT devices.

5.3.1 Average Packet Success Probability

As discussed, the essential performance metric in IoT networks is the success probability of a message. The small size of the messages transmitted by the nodes allows their encapsulation into single packets, which are possibly transmitted multiple times as MAC layer frames. Since we are interested in the overall performance of the MAC layer, in Figure 5.1 we present the average packet success probability of the CSMA No Ack protocol, calculated for different numbers of contending nodes and different values of the CCA threshold. In order to measure the efficiency of the CCA technique, we show in the same figure the results obtained by the Aloha No Ack protocol. For both protocols, the number of retransmissions K is set at 3.

We can see from the simulation results that the cell average PSP depends on the value of the CCA threshold parameter. It is clear that for the lowest value of -95 dBm we get the best performance since the node sensitivity is very high, which makes the MAC layer able to avoid more collisions than for higher values of the CCA threshold, where the problem of hidden node is more present, which explains the drop of the PSP performance when we increase the CCA threshold value.

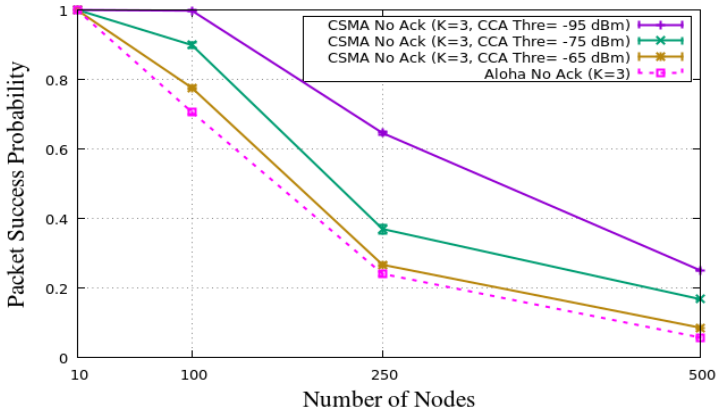


Figure 5.1 : Packet success probability for CSMA No Ack with different values of the CCA threshold

. If we want to compare between the CSMA No Ack protocol and the Aloha No Ack protocol, we need to be more precise about the CCA threshold, since this could lead to totally different conclusions. CSMA No Ack with a CCA threshold of -95 dBm is clearly having better PSP results than Aloha No Ack, with 40% of difference for the case of 250 nodes. CSMA No Ack with a CCA threshold of -75 dBm is also performing better than Aloha No Ack, with a gain of 20% almost all the time. However, when a CCA threshold of -65 dBm is used, the results are only slightly better than Aloha No Ack and we can barely see the impact of the carrier sense mechanism.

5.3.2 Average node activity time

As explained, in this work we do not directly compute the node energy consumption, but we calculate a correlated metric instead: the duration each node spends in an active ON state, i.e. the time the node is using its radio module, either for transmission, reception or listening the channel. For the CSMA No Ack access scheme, we consider that the node is active in order to sense the channel during the back-off slots, as well as during the transmission, while for the Aloha No Ack access scheme, the node is considered active only during the transmission. Figure 5.2 shows the cell average On time for the CSMA No Ack solutions and for the Aloha No Ack one, for different node densities.

The results show that, for the CSMA No Ack solutions, the lower the CCA threshold, the higher the On time period. This is due to the increased sensing area of the node, which makes it spend more time sensing and waiting for the channel to be free, in other words resulting in bigger back-off periods. We can notice that the CSMA No Ack with a CCA threshold of -95 dBm and CSMA No Ack with a CCA threshold of -75 dBm are getting almost the same On time period for medium and high density networks. Meanwhile, CSMA No Ack with a CCA threshold of -65 dBm is showing the best energy results of the three, especially in a medium density network.

In order to compare between the CSMA solutions and the Aloha one in terms of activity time, it is very clear that the Aloha No Ack On time is very short and it is performing better than all the CSMA No Ack versions, including the one with a CCA Threshold of -65 dBm which gave similar performance in terms of PSP. We can also notice that the Aloha activity time is practically constant and that is because the nodes in this case are awake only for sending the packets, so the average On time is always the same, independently from the network density, and only depends on the number of repetitions *K*, which we proved already in Chapter 3.

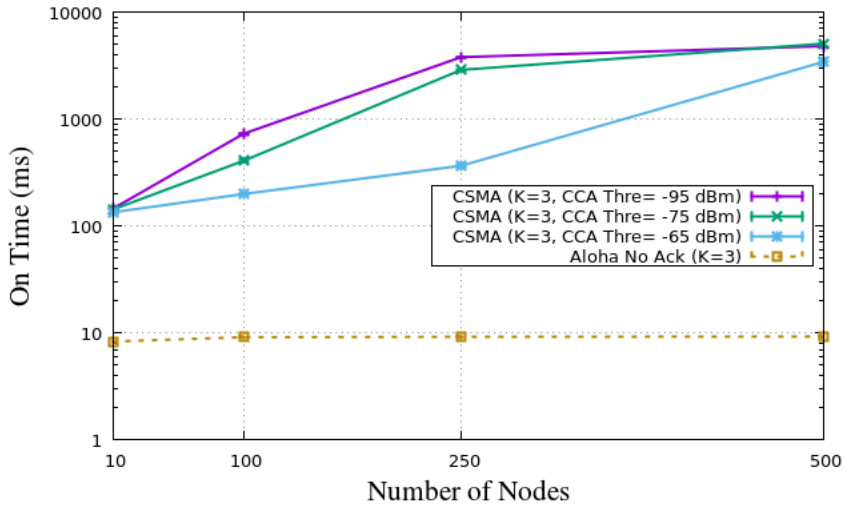


Figure 5.2 : Average node ON time for CSMA No Ack with different values of the CCA threshold

Finally, if we consider the PSP results along with those for the On time, we can say that the CSMA techniques are indeed better than Aloha in terms of PSP results, but only if the IoT devices have a good sensitivity (a low CCA threshold). However, carrier sensing brings worse results in terms of On time, hence a higher energy consumption, which is not a very welcome feature in many IoT applications. However, it could still be interesting for certain applications to trade off higher energy consumption for higher PSP. Nevertheless, if the CSMA No Ack protocol functions with a low sensitivity (a high CCA threshold value), the PSP will be only slightly higher than for Aloha No Ack, while resulting in a much longer On time. In this case, it is hard to say that it is worthy to add a carrier sense functionality for many IoT applications, the small PSP gain not justifying the much higher energy consumption.

5.3.3 Individual packet success probability

We investigate a little bit deeper the impact of the CCA threshold on the performance of CSMA No Ack. In Figure 5.3, Figure 5.4 and Figure 5.5, each point corresponds to a node of the network and we show the PSP obtained by each node, as well as its CCA conflict ratio. We also show the network average PSP; just like in the previous section, we continue using the same three values for the CCA threshold . However, we inhere focus on networks with a different number of nodes: 100, 250 and 500 nodes, which we respectively denote as a low-dense, medium-dense and high-dense network.

We notice the same thing as in the previous subsection for all network densities: the average PSP drops when the CCA conflict rate increases, and we also notice that there is a sort of a correlation between the CCA conflict rate of a node and its PSP result, especially in the case of a CCA threshold of -75 dBm. This feature is present too for a network with a CCA threshold of -65 dBm, but it is less visible, while it is absent with a CCA threshold of -95 dBm, where all the nodes of the network have the same CCA conflict rate value of 1.

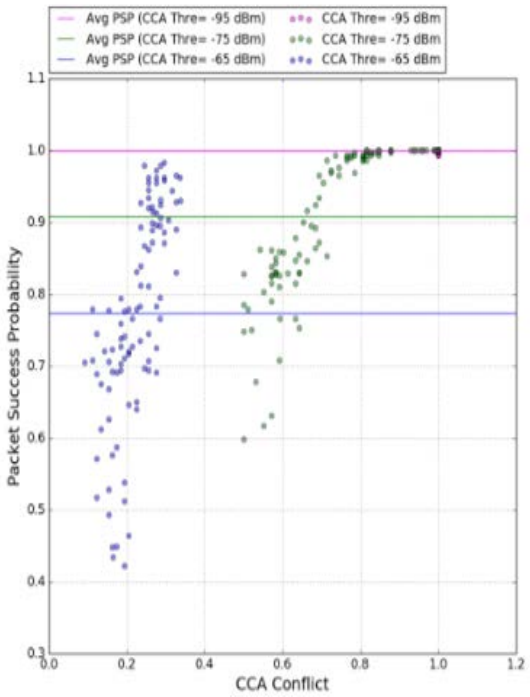


Figure 5.3 : Packet success probability for a network of 100 nodes

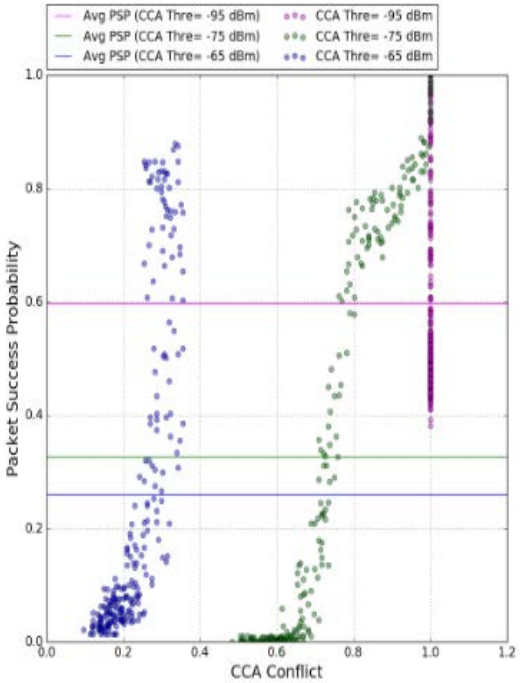


Figure 5.4 : Packet success probability for a network of 250 nodes

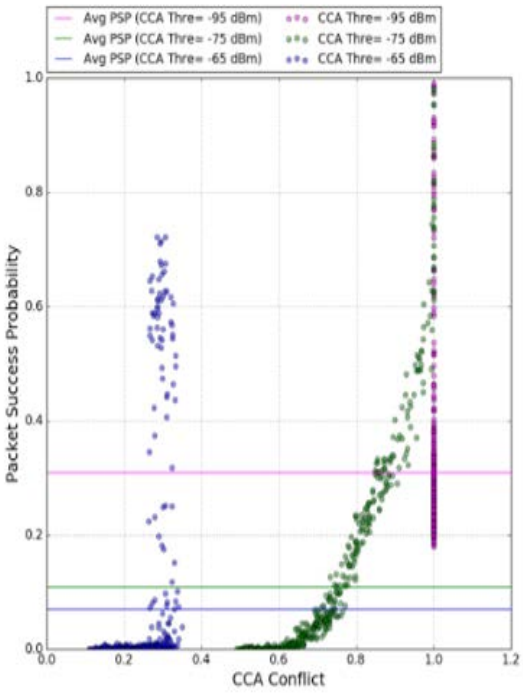


Figure 5.5 : Packet success probability for a network of 500 nodes

The other interesting behavior with respect to the CCA threshold modification is the difference of the PSP range of values: for a medium-dense network all the PSP values are between 38% and 100% for a CCA threshold of -95 dBm, while this range is from 0% to 100% for a CCA threshold of -75 dBm and between 0% and 85% for a CCA threshold of -65 dBm. We also remark that, for a medium-dense network with a CCA threshold of -65 dBm, there are 30% less nodes reaching a PSP lower than 1%, compared to the case of a -75 dBm CCA threshold, even though the maximum PSP is limited to 85% in the former case. However, the average PSP is higher for a CCA threshold of -75 dBm than in the case of -65 dBm. This observation is seen only for medium-dense networks; for other densities, the lower values of the CCA threshold also bring more fairness in the range of PSP results.

We consider that the two highest values of the CCA threshold (-65 dBm and -75 dBm) are the closest to a CSMA protocol applied in a real IoT network, while the CSMA with a CCA conflict rate of 1 for all nodes (meaning that each node hears all the other nodes of the cell) is practically impossible to obtain in a real implementation.

Meanwhile, the Aloha based solutions are giving a CCA conflict rate of 0 all the time, reaching a PSP a little bit worse than the CSMA No Ack with a -65 dBm CCA threshold. The Aloha No Ack PSP range of values is different to the CSMA No Ack solutions: we notice that the maximal value of PSP for Aloha No Ack is almost 20% lower than the one given by CSMA with a -65 dBm CCA threshold, except for a low dense network where the difference is only of 10 %. This could be another advantage of the CSMA No Ack solution over Aloha No Ack, but the difficulty of implementing a high sensitive CSMA solution in a real IoT network is still a big challenge.

5.3.4 Individual node activity time

In Figure 5.6, Figure 5.7 and Figure 5.8, we show the On time obtained by each node of the network and its CCA conflict rate. We also show the network average On time and, just like in the previous sub-section, we focus on networks of 100, 250 and 500 nodes, which respectively represent a low-dense, medium-dense and high-dense network.

We notice that, in all network densities, the average On time gets higher when the CCA conflict rate increases. We notice as well that there is a sort of a correlation between the CCA conflict rate of a node and its On time. Finally, we observe that the lower the CCA threshold, the more On time we spend on average and the wider the On time range. This is due to the larger detection zone of the node, which implies more time spent sensing the channel during busy periods.

The Aloha No Ack protocol is much more efficient energy wise, since it is getting a very short and constant On time period for all network densities. This important difference of the activity time between Aloha and CSMA solutions it a key advantage for Aloha in the case of IoT network applications.

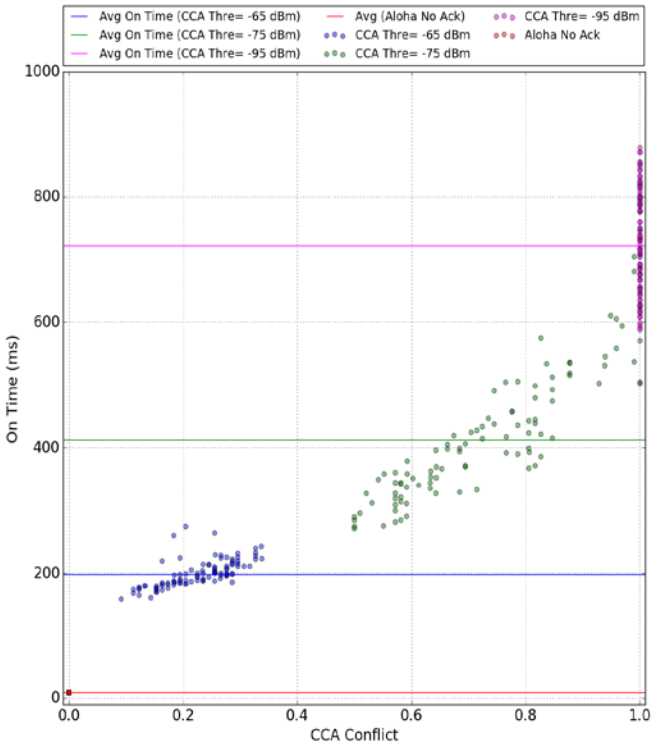


Figure 5.7 : Node activity time for a network of 100 nodes.

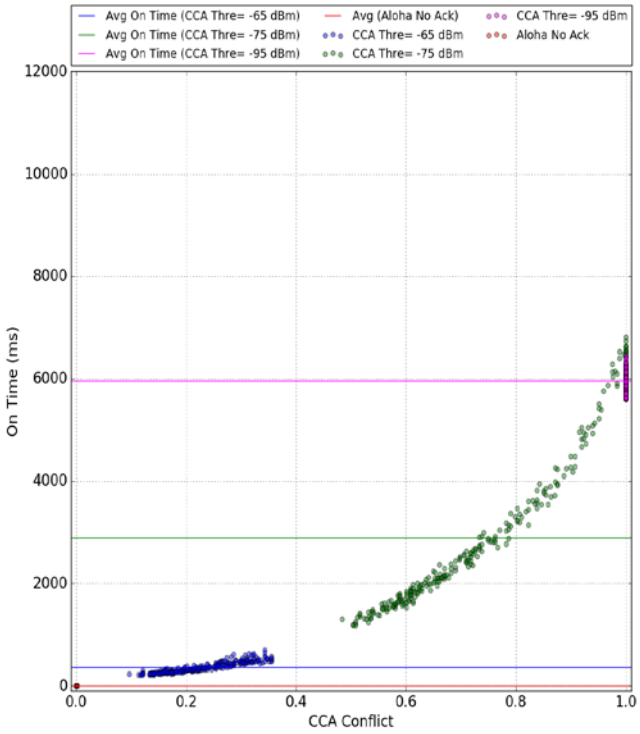


Figure 5.6 : Node activity time for a network of 250 nodes.

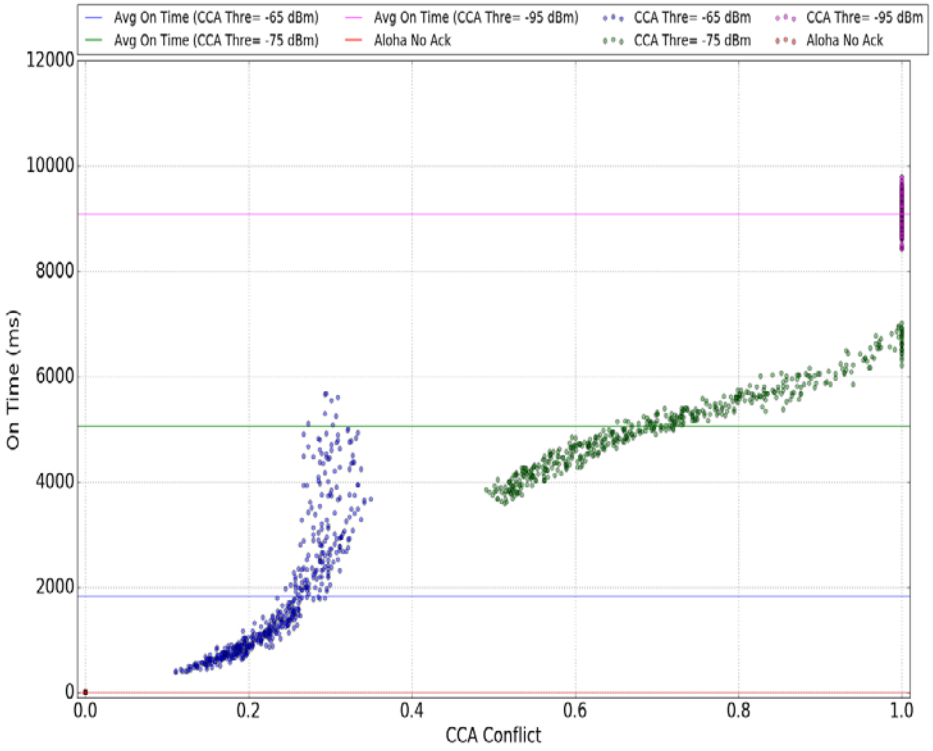


Figure 5.8 : Node activity time for a network of 500 nodes.

5.4 Impact of the number of retransmissions

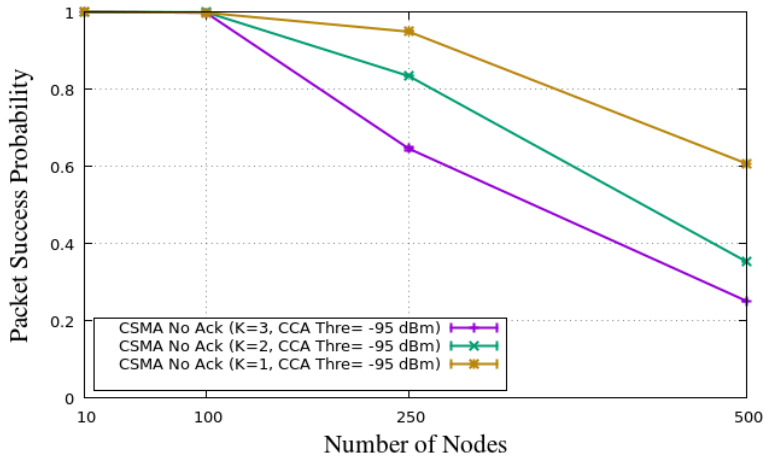


Figure 5.9 : Packet success probability for a CCA threshold of -95 dBm

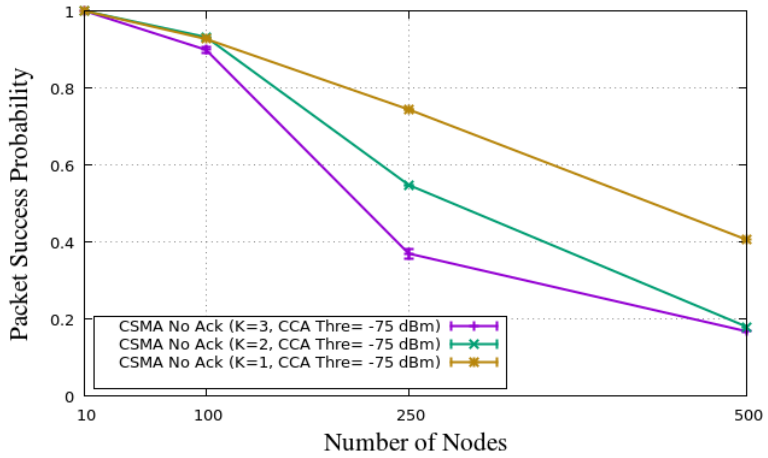


Figure 5.10 : Packet success probability for a CCA threshold of -75 dBm

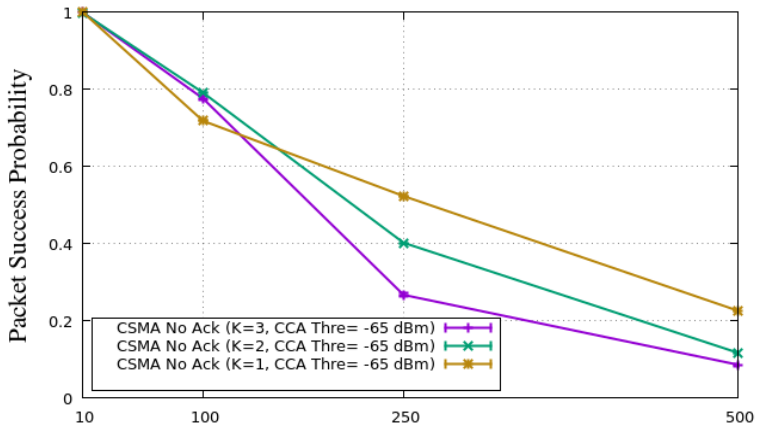


Figure 5.11 : Packet success probability for a CCA threshold of -65 dBm

In Figure 5.9, Figure 5.10 and Figure 5.11, we show the PSP results for networks using different CCA threshold values, with the focus in here on the impact of the frame retransmission number (*K*).

We notice that for all CCA threshold values and for the majority of network densities, the best PSP performance are obtained by the lowest frame retransmission number, i.e. $K = 1$. The network with $K = 1$ reaches a better PSP performance by more than 20% with respect to networks with higher *K* value, *i.e.* for high-dense networks with CCA thresholds of -75 and -95 dBm. This phenomenon can be explained with the same arguments presented in the previous chapter for the superiority of the Aloha No Ack network with $K = 1$: the main reason is that retransmitting less makes the probability of collision decrease and enhances the channel quality.

There are two exceptions for the higher performance of networks with $K = 1$: in Figure 5.10, we see that for a network of 100 nodes, the configurations with $K = 2$ and $K = 1$ are providing the same PSP result, and in Figure 5.11 we observe that the two higher *K* values are having a better PSP of nearly 10% than the configuration with $K = 1$, in the case of a network of 100 nodes.

We then study the energy consumption behavior while changing the frame retransmission number for the same CCA threshold values as above. Figure 5.12, Figure 5.13 and Figure 5.14 show the On time results for each CCA threshold value for different frame retransmission numbers. We remark that networks with $K = 1$ are the best energy saving networks, whatever the CCA threshold value. The On time is at least ten time shorter for networks with $K = 1$ than for networks with higher *K* values. In Figure 5.13, for a CCA threshold of -75 dBm and a high-dense network of 500 nodes, the CSMA No Ack with $K = 1$ has an On time of 181 ms, the configuration with $K = 2$ has an average On time of 1866 ms, while with $K = 3$ the network reaches the average of 5065 ms On time.

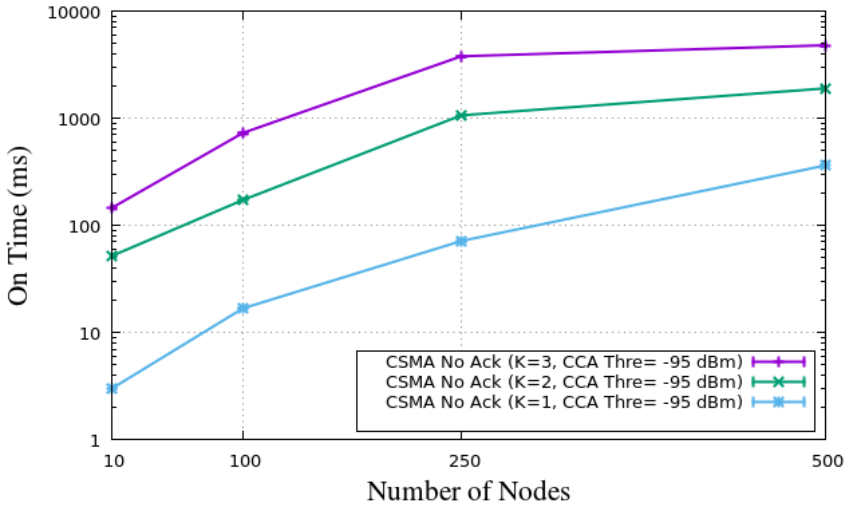


Figure 5.12 : Node activity time for a CCA threshold of -95 dBm.

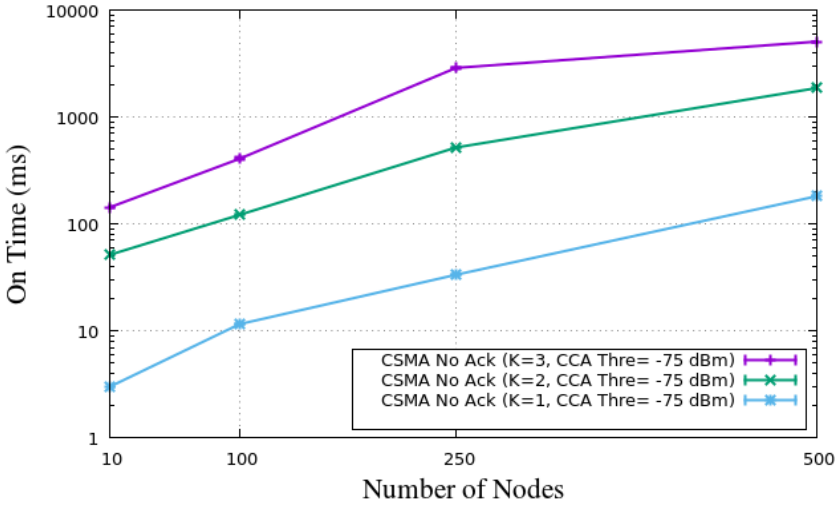


Figure 5.13 : Node activity time for a CCA threshold of -75 dBm.

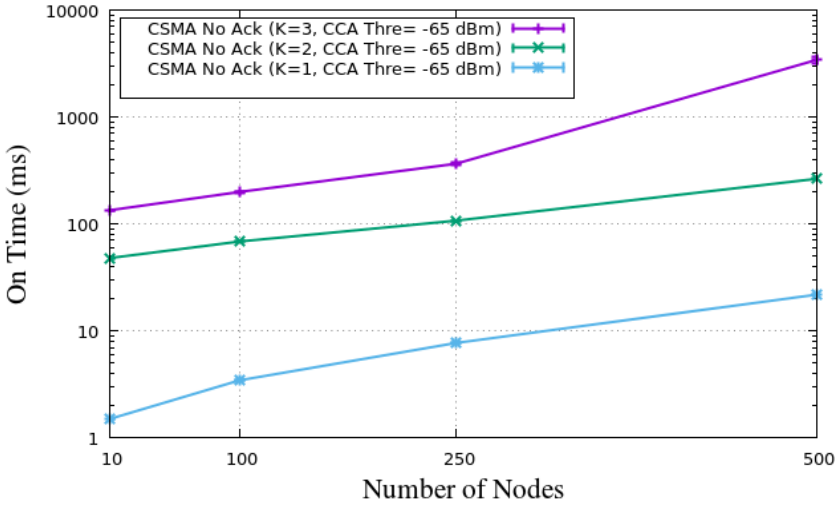


Figure 5.14 : Node activity time for a CCA threshold of -65 dBm.

5.5 Optimal number of retransmissions for CSMA No Ack

In this section we proceed similarly to Chapter 4 and find the optimal frame retransmission number for each network condition. We note that the choice of optimal K in this chapter is based only on simulation results the possible radio propagation errors are simply a consequence of the propagation model used in ns3.

Figure 5.15 shows the optimal value of K for each CCA threshold value: we can see that the optimal K is 1 for almost all network densities and all CCA threshold values. This is because, for small networks, all the K values, including $K = 1$, result is almost perfect PSP, while for large networks the reduced number of retransmissions decreases the channel contention. However, we notice the existence of an exception for networks between 100 and 250 nodes, where the optimal $K = 2$ once the CCA threshold is no longer ideal.

We have to mention that these optimal K values are obtained while considering only the PSP results, to respect the same methodology as in the previous chapter. This is coherent with the context of the previous chapter, where Aloha No Ack was used and the energy consumption is not problematic in the case of that MAC protocol. However, the CSMA based networks suffer from higher energy consumption. Therefore, we have to consider the On time results and make the choice of optimal K based on the compromise between PSP and On time results. Then, with a simple observation of the

PSP results along with the On time results, the optimal *K* would always be *K* = 1, for all network densities and CCA threshold values.

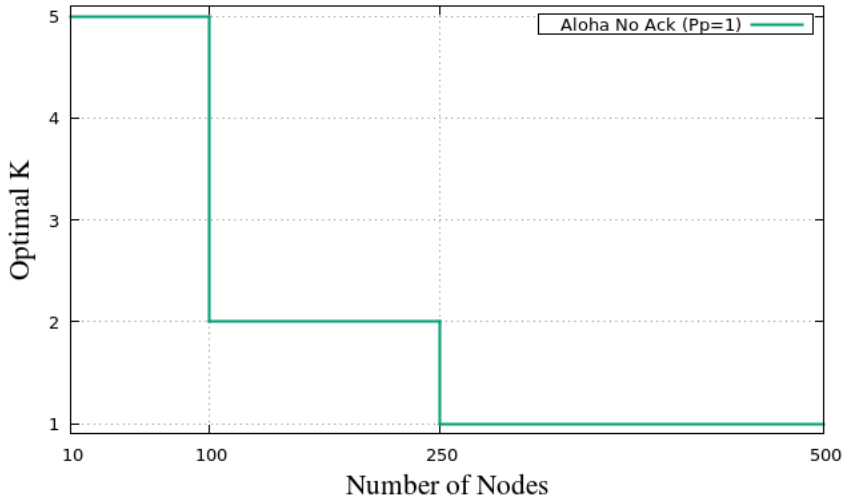


Figure 5.15 : Optimal value of K for different CCA threshold values.

5.6 Comparison under optimal settings

In this section we compare the result obtained by an Aloha No Ack based network using the optimal *K* values and the result obtained for a CSMA No Ack based network using the optimal *K*. This helps us to evaluate the impact of adding a carrier sense mechanism to an LPWAN network. In order to have a CSMA No Ack implementation that is realistic and that keeps offering an enhancement to the Aloha reliability results, we note that we focus in here on CSMA No Ack with the CCA threshold of -75 dBm.

x

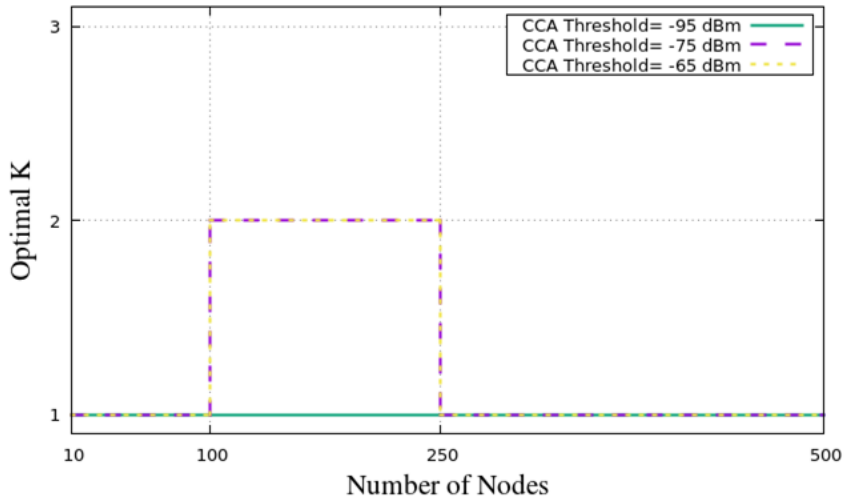


Figure 5.16 : Optimal K value for Aloha No Ack with Pp=1.

Figure 5.16 shows the optimal *K* values for Aloha No. This study included from 1 to 5 frame retransmissions, as explained in the previous chapter. For CSMA No Ack, we know that the optimal value of *K* (denoted K_{opt}) is always 1, and we try to check in here if sending only one frame with carrier sense activated is better than sending more frames without any carrier sense mechanism.

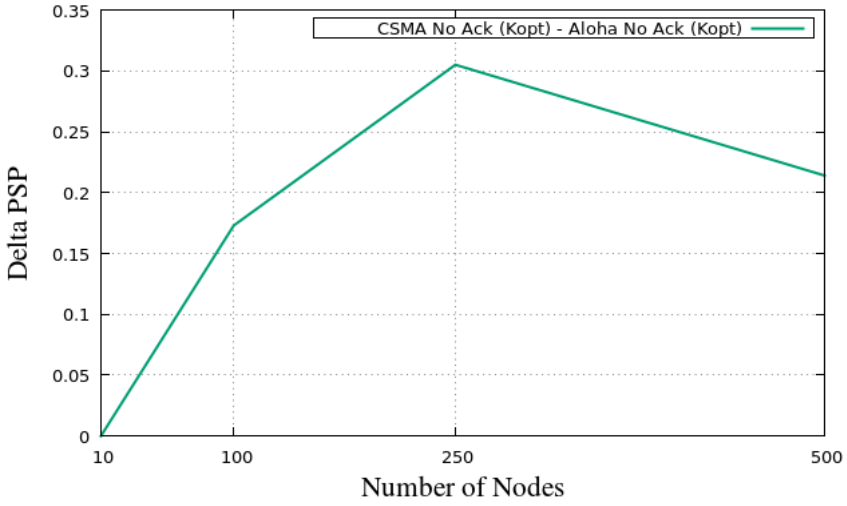


Figure 5.17 : PSP gain obtained by CSMA No Ack with respect to Aloha No Ack

In Figure 5.17, we show the difference in terms of PSP results obtained by CSMA No Ack with K_{opt} and the reliability results obtained by Aloha No Ack with K_{opt}. As shown in the figure, the PSP obtained by the CSMA solution is always higher than the one obtained by the Aloha one, with the exception to the low dense network of 10 nodes where both MAC solutions obtain the same PSP result. For a medium-dense network, of 250 nodes, the difference reaches 30% and for a high dense network, of 500 nodes, the enhancement is of 21%.

As we know the increased energy consuming feature of the CSMA based network, it is clear that this enhancement in reliability compared to Aloha No Ack will bring an extra energy cost. Therefore, we present in Figure 5.18 the difference of the On time periods obtained by both solutions. We see in this figure that, in the majority of the cases, the CSMA based solution has longer On time periods, with the exception of a low-dense network of 10 nodes. For this latter case, the optimal *K* for the Aloha based solution has the value of 5, while the CSMA optimal *K* is always 1. Therefore, in a low density network, sending one frame with carrier sense allows us to reach the same PSP as sending five frames without carrier sense, while also saving energy.

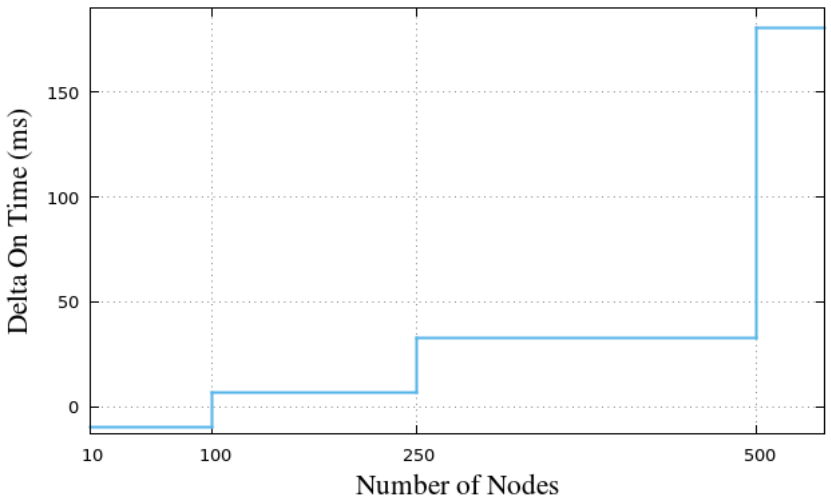


Figure 5.18 : Extra activity time produced by CSMA No Ack with respect to Aloha No Ack

We see in Figure 5.18 that the energy cost brought by CSMA No Ack increases with the number of nodes. This is due to the higher time spent by the nodes to wait for the channel to be free when more nodes are accessing the channel.

In order to evaluate the advantage of a solution compared to another we need to look at the difference in terms of both PSP and activity time. For a network of 100 nodes, using CSMA No Ack with K_{opt} enhances the PSP by 17% and makes the On time longer of 7 ms, which seems as a small cost for an acceptable reliability enhancement. For a network of 250 nodes (medium-dense), using CSMA No Ack with K_{opt} enhances the PSP by 30% and makes the On time longer by 32 ms, which could be a reasonable cost for such a significant reliability enhancement. However, in the case of a more dense network, of 500 nodes for example, the enhancement of PSP is of 21% and the On time cost is of 180 ms, which could be considered as a big cost, even prohibitive in energy-constrained scenarios.

5.7 Conclusion

In this chapter, we studied the implementation of the CSMA No Ack MAC protocol in an LPWAN context. Our study focused on the CCA threshold; we showed with simulation results how this parameter impacts the network performance significantly in terms of packet success probability and node activity time.

Then, we introduced the CCA conflict rate, a node level metric which reflects directly the percentage of contenders that the node is able to hear, which allows us to deduce the percentage of hidden terminals for each node. Afterward, we showed the correlation that exist in the majority of the cases between the CCA conflict rate and the performance metrics (PSP and On time). Moreover, we conducted a study on the impact of the frame retransmission number on the network performance, similarly to what we did in the previous chapter for Aloha No Ack based networks. We remarked that, for all CCA threshold values, when no frame retransmission is used ($K = 1$), the network performed better in terms of PSP and On time, hence the $K = 1$ represents the optimal K for CSMA No Ack. Finally, we provided a comparison between Aloha No Ack with optimal K and CSMA No Ack with optimal K, and we showed how CSMA No Ack has better PSP all the time, but with longer On time period. We also showed how sometimes a good compromise can be achieved when using CSMA No Ack with $K = 1$.

To the best of our knowledge, this is the first contribution that considers the CCA threshold impact while studying the implementation of a CSMA-based protocol for LPWANs. And this is the first work that introduces the CCA conflict rate and proposes a realistic implementation of CSMA, that could present a good compromise between PSP and On time compared to Aloha based network.

6. A Machine Learning based MAC Protocol

In this chapter, we present our contribution that uses a machine learning algorithm, which is based on Convolutional Neural Networks (CNN), to propose a cognitive MAC solution for dedicated IoT networks. The strength of our contribution consists of studying the local condition of every node in order to propose the optimal MAC layer configuration per node. The optimal MAC configuration per node would lead us to an optimal overall performance of the network. The coexistence of different MAC solutions within the same cell is allowed, which represents another originality of our contribution.

The rest of the chapter is organized as follows: in Section 6.1 we investigate the coexistence of MAC protocols in the IoT cell without any machine learning guidance. In Section 6.3, we explain our machine learning based MAC solution. In Section 6.4, we first validate the machine learning predictions with simulation results and then we show how we integrate the machine learning solution in the simulator. In Section 6.5, we present simulation results obtained with the cognitive MAC solution based on the CNN algorithm.

6.1 Coexistence of MAC protocols

The dedicated IoT network cell coverage could reach more than 10 km. Within this surface, the network condition will likely not be uniform. Then, clearly nodes will not have the same requirements at the MAC layer. Therefore, we believe that a single ideal MAC solution for all nodes is far from being realistic. Therefore, we develop a solution that dynamically adapts the MAC layer configuration, in order to fit the current network condition and the local requirements of a node. Our solution is capable to provide a customized MAC configuration for each node, which enhances the node performance and the overall performance of the network. Hence, nodes can have different MAC configurations due to their different requirements. Some contributions in the literature investigated the possibility of using different MAC protocols for nodes belonging to the same network. Daniel and Andrea [62] discussed the coexistence of Aloha and CSMA within the same IoT cell. The authors show how Aloha nodes are not impacted by the increase of nodes using CSMA, while the CSMA nodes suffer from performance degradation. This performance degradation for CSMA nodes is due to less access to the channel when Aloha nodes are present, because they are more frequently blocked by the CCA mechanism. We can then conclude that MAC protocol coexistence is tricky and could create a fairness issue between nodes. However, authors in [13] only considered the case where a single frame is sent by the MAC layer, the acknowledgements and the frame retransmission were not allowed for modeling simplifications.

In this section, we study the coexistence of Aloha No Ack and CSMA No Ack in order to see how it impacts the performance in terms of packet success probability and energy consumption. As in the rest of this work, we use the ns3 simulator to conduct this study.

For the remainder of this chapter, we consider only the CSMA No Ack with a CCA threshold of -75 dBm, and we consider only MAC solutions without acknowledgement messages. The choice of -75 dBm was done for realistic reasons, since the CCA conflict ratio values are close from what we can expect in a real deployment, going from 40% to 100%. For this subsection, the simulation results are obtained using 3 retransmissions for both MAC protocols.

Figure 6.1 shows the PSP of each node and its distance to the gateway, for a high-dense network of 500 nodes, in the case of a homogeneous MAC configuration, where only one of the protocols is used. We chose this high density network for our tests, because the baseline performance of the two solutions is low, and we want to see how much we can improve this. We will also test other network densities in the following.

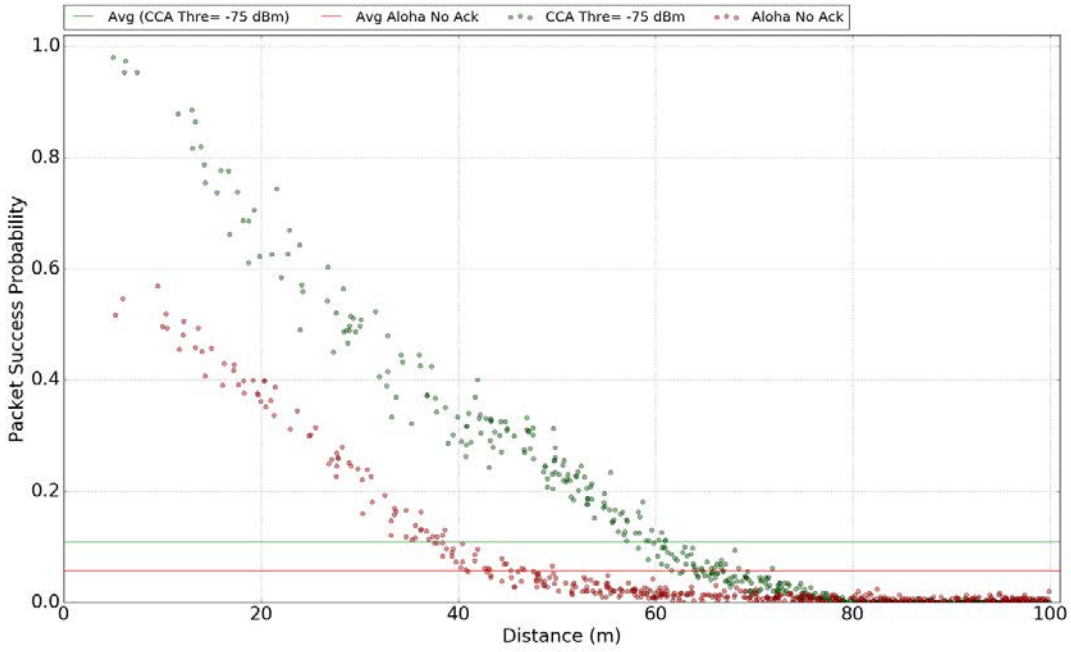


Figure 6.1 : Node PSP and its distance to the gateway.

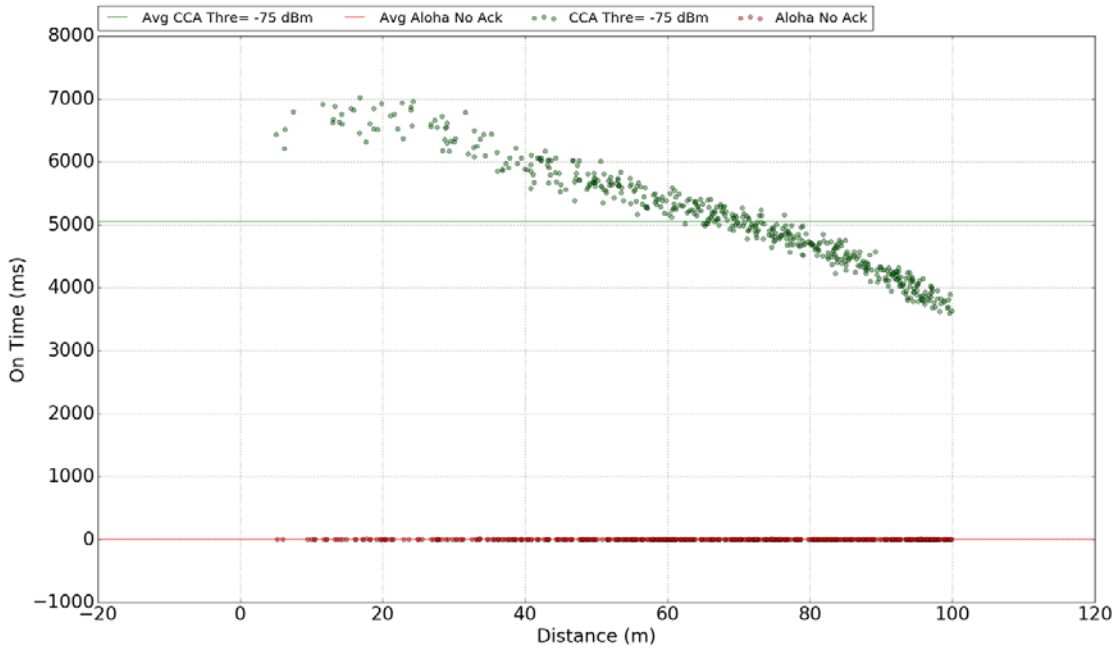


Figure 6.2 : Node ON Time and its distance to the gateway.

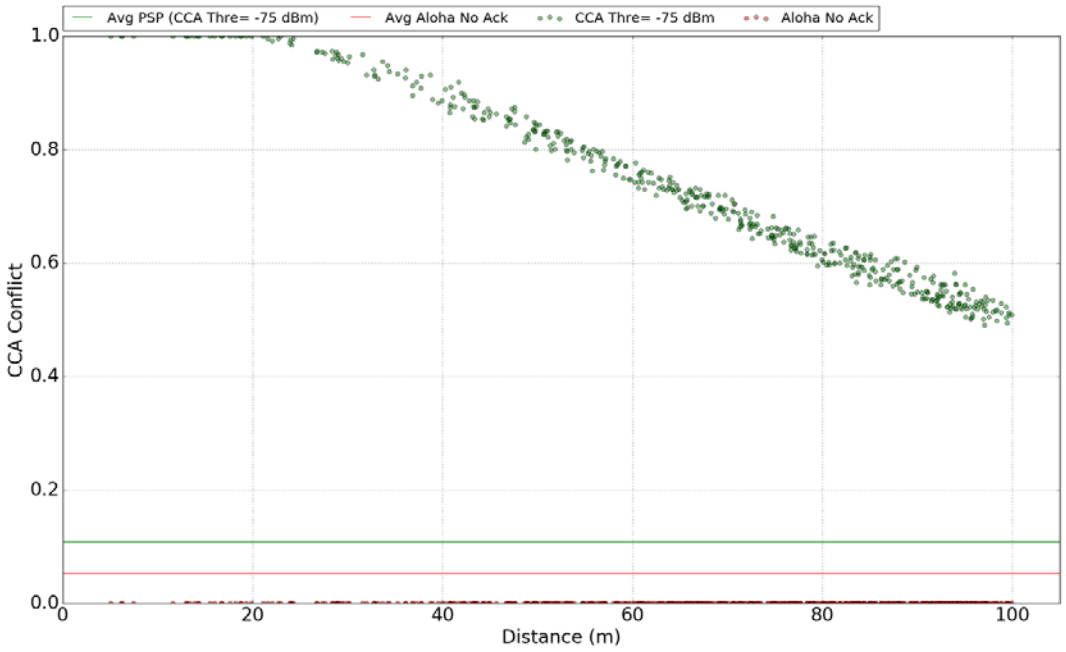


Figure 6.3 : Node CCA Conflict and its distance to the gateway.

We can observe that, for both protocols, Aloha No Ack and CSMA No Ack, the further the node is from the gateway, the less PSP it obtains. For the CSMA No Ack network, the nodes which are closer to the gateway are the ones with higher CCA conflict ratio (see Figure 6.3), which reflects in their higher capacity to avoid collisions, enabling them to have good PSP performance.

Figure 6.2 shows the energy consumption of a node and its distance to the gateway. The Aloha No Ack On time is very short, constant and independent from the distance between the sender node and the gateway. Meanwhile, for CSMA No Ack, the On time is longer for the nodes that are closer to the gateway, and that is because they have higher CCA conflict ratio (see Figure 6.3). This results in longer carrier sense periods before accessing the channel. For further nodes, the CCA conflict rate is smaller, which makes them certainly less immune to collisions, but allows them to access to the channel faster.

In Figure 6.1 we notice that, starting from the distance of 70 meters, the PSP results of both protocols are pretty similar. Hence, the intuition is that, if we configure the nodes situated further than 70 meters to use Aloha No Ack, then no big changes to the PSP results will occur. At the same time, the nodes that use Aloha No Ack will have shorter On time, which will improve the average energy consumption of the network.

Figure 6.4 and Figure 6.5 show the results of a heterogeneous network, where we have some nodes using Aloha No Ack and others using CSMA No Ack as a MAC protocol. We denote this as hybrid solution. As previously explained, we use Aloha No Ack for nodes that are situated further than 70 meters from the gateway, while the rest of the nodes are using CSMA No Ack. In Figure 6.4, we show the PSP results for the hybrid solution: we notice that the average PSP results is almost the same as the PSP result obtained by a homogeneous Aloha No Ack configuration, which means a degradation of performance compared to CSMA No Ack. We remark that the nodes using the Aloha No Ack did not face any change in term of PSP result, while for the CSMA No Ack nodes we see a big drop of PSP results, since they have less access to the channel because of the Aloha No Ack nodes. The Aloha No Ack nodes access freely to the channel, without any blocking CCA mechanism. The PSP drop is not distributed uniformly among the CSMA No Ack nodes, as it depends on the CCA conflict ratio of the node. As shown in Figure 6.6, the nodes with the highest CCA conflict ratio are nodes with a small distance to the gateway, which are the nodes that faced a big degradation of performance for the hybrid solution.

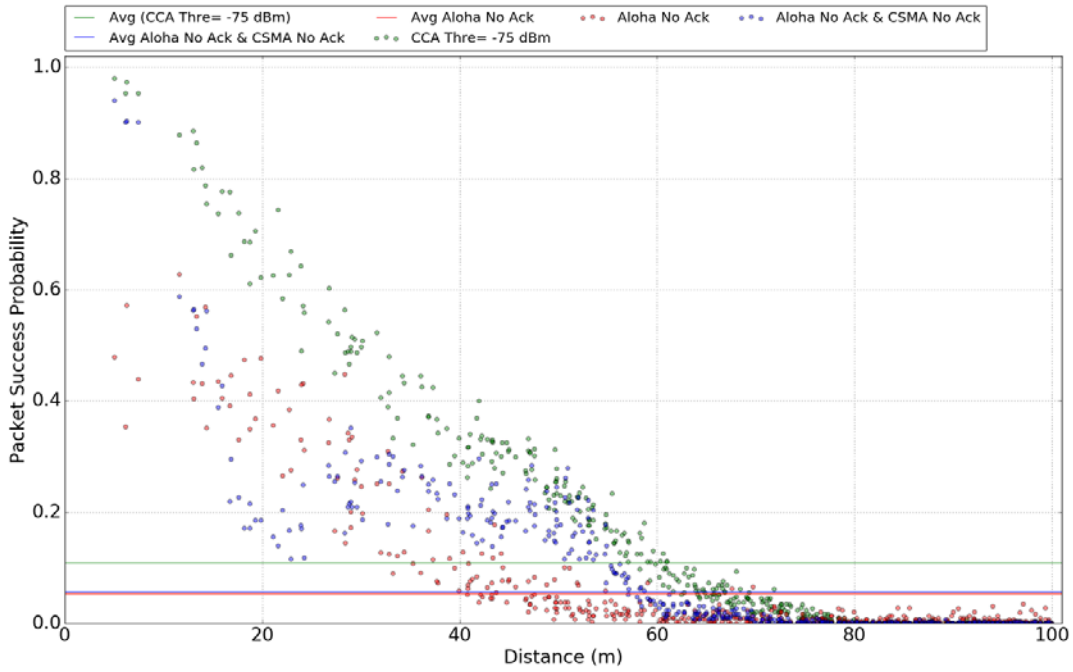


Figure 6.4 : Node PSP and distance to gateway for heterogeneous networks.

Figure 6.5 : Node ON Time and distance to gateway for heterogeneous networks.

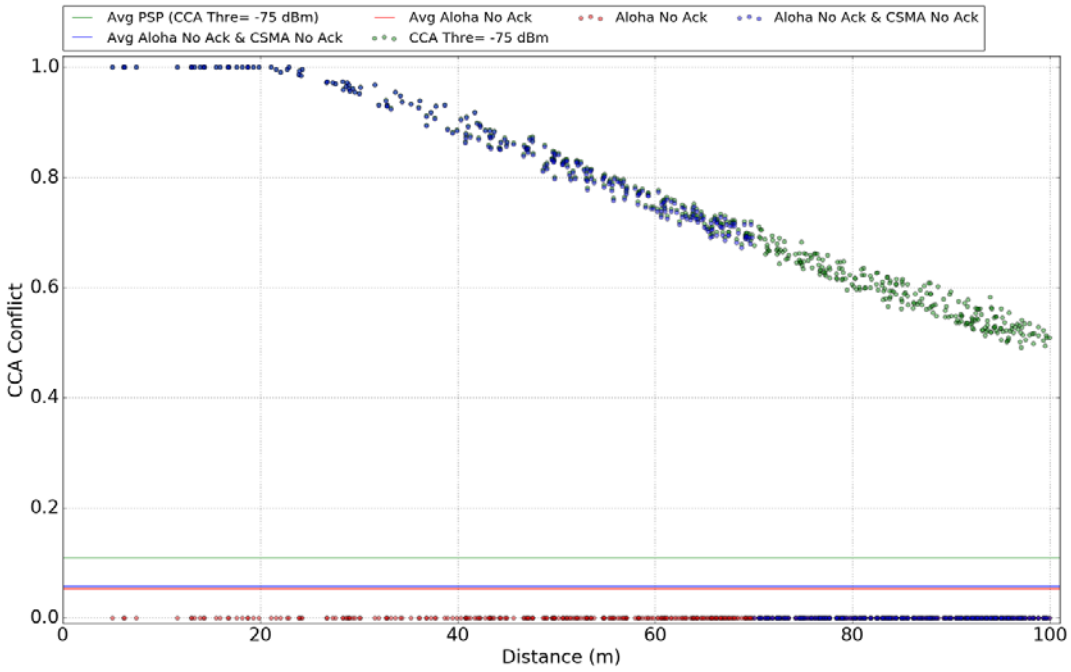


Figure 6.6 : Node CCA Conflict and distance to gateway.

For the energy consumption, it was logic to expect shorter ON time period for the hybrid network than for a CSMA No Ack network. However, in Figure 6.4, we remark that the ON time result for a hybrid network is the worst: the average is almost the double compared to the CSMA No Ack network. The range of values is enormous and goes from tens to thousands of milliseconds. These results confirm the observations done for the PSP results: the Aloha No Ack nodes are getting a negligible ON time duration, but the CSMA nodes are blocked by the unfriendly Aloha traffic.

The results in this section lead us to conclude that the coexistence of Aloha No Ack and CSMA No Ack protocols within the same IoT cell is more complicated than we expected. This coexistence actually degrades the network performance in our example. Therefore, in the next sections we will show how a machine learning algorithm, based on CNN, enables us to transform the MAC protocols coexistence in an advantage, by proposing a cognitive MAC solution.

6.2 Machine Learning Algorithm

Through this section, we show how a machine learning algorithm is able to predict network performance based on MAC layer parameters and provide us with a suitable MAC configuration distribution for a given network situation. In this chapter, the network situation consists of the number of nodes, traffic intensity and the nodes distribution among the cell. The proposed machine learning based solution is also capable to build on MAC protocols coexistence and enhance the MAC layer performance.

In a dedicated IoT context, changing the value of a key MAC parameter changes the MAC layer configuration and even the behavior of the MAC protocol. For example, the difference between Aloha and CSMA might appear huge, while at the implementation level only two parameters need to be changed to switch between the two protocols: the CCA threshold and the back-off window size. Even for the same MAC protocol, different set of configurations can be achieved by changing other MAC layer parameters, such as the frame retransmission number, or even the use of acknowledgement messages.

Different categories of machine learning algorithms exist and, inside each category, plenty of versions and implementations are possible. To start with, we discuss the two major machine learning

categories: unsupervised and supervised machine learning. The unsupervised algorithms are used when we have a lot of data to exploit, which is not labeled. Then, the unsupervised algorithm is used to discover the structure of the data and to help finding unknown patterns in data. To the contrary, supervised learning algorithms are trained with labeled data. The algorithm target here is to model correlations and dependencies between the output and the input. During the training phase, we provide the algorithm with real output, then the algorithm makes predictions and corrects itself based on the real output. This learning is repeated until the algorithm reaches an acceptable accuracy of prediction. Afterward, we can use the algorithm to predict output for newly data.

In our scenario, we aim to exploit the network history in order to learn about the network performance evolution through the change of several parameters. The network history that we have is the data generated by the simulations; this data contents are the MAC layer configuration of each node, the network density and the obtained PSP and ON time, on average and per each individual node. The MAC configuration is represented by the setting of the MAC layer parameters. Hence, the data is already pre labeled, which made us tend more for supervised algorithms. Moreover, thanks to our previous chapters' contributions, we have identified key parameters in our system, that represent the main labels or features of the learning algorithm input data. Our evaluation metrics, PSP and ON time, will represent the output data for the algorithm.

We choose to use neural network algorithms for supervised learning. We firstly used a feedforward artificial neural network (ANN) Multilayer Perceptron (MLP) algorithm [91-92]. We did an exhaustive test phase where we tried different MLP architectures. After this phase, we did not reach a satisfying accuracy rate.

We then turned towards a Convolutional Neural Network (CNN) solution [93-95] and, after an exhaustive test phase, the algorithm accuracy reached 95%, which represents an acceptable result in our opinion. Our CNN architecture is composed of three layers: input layer, hidden layer and output layer. The input layer is composed of twelve neurons, the hidden layer of eight neurons and the output layer of two neurons. The two neurons of the output layer represent, respectively, the predicted PSP and the predicted ON time.

The epoch is an important parameter for the CNN algorithm. A CNN epoch finishes when the entire dataset is passed forward and backward through the neural network. As we need to pass the full dataset multiple times to the same neural networks, until a good accuracy is reached, the optimal number of epochs depends on each dataset. After the test phase we notice that the accuracy is stable for epoch values larger than 50.

We inhere show that the use of a CNN guides us to distribute the MAC configurations per node. To do so, we start by training the CNN algorithm with data generated by simulations. The data were introduced to the CNN algorithm as input and output data; every input line represents a node configuration and every output line represents a node PSP and ON time results. The MAC configuration is defined by the distance separating the node from the gateway, the number of retransmissions, the CCA conflict ratio and the number of nodes. These parameters are chosen based on our previous contributions; we consider them as key parameters.

We fed the algorithm with data from different simulations. We noticed that the accuracy rate of the CNN is better when the number of nodes is the same between training data and the new data to predict. For example, to predict the MAC configuration for a network of 500 nodes, we train the CNN with data for networks of 500 nodes.

Figure 6.7 shows the CNN predicted results in terms of PSP and simulation results, for Aloha No Ack and CSMA No Ack protocols, and for different network densities, going from low dense network to high dense network. The simulation results are shown with confidence interval of 95% and the prediction results are averages of 10 predicted results. Figure 6.7 shows that the predicted PSP are similar to the simulated results, which validates the accuracy of our CNN model.

The CNN prediction algorithm is then used as base to develop an optimization solution, which provides the MAC configuration per node. The optimization algorithm takes as input the number of nodes and the traffic intensity of the network we want to study. Then, the algorithm predicts PSP and ON time results for all possible MAC configuration distributions. Afterward, the algorithm compares

between these predicted results and picks the best MAC solution. We are interested in MAC configurations that provide a good compromise between PSP and ON time per node and for the entire network.

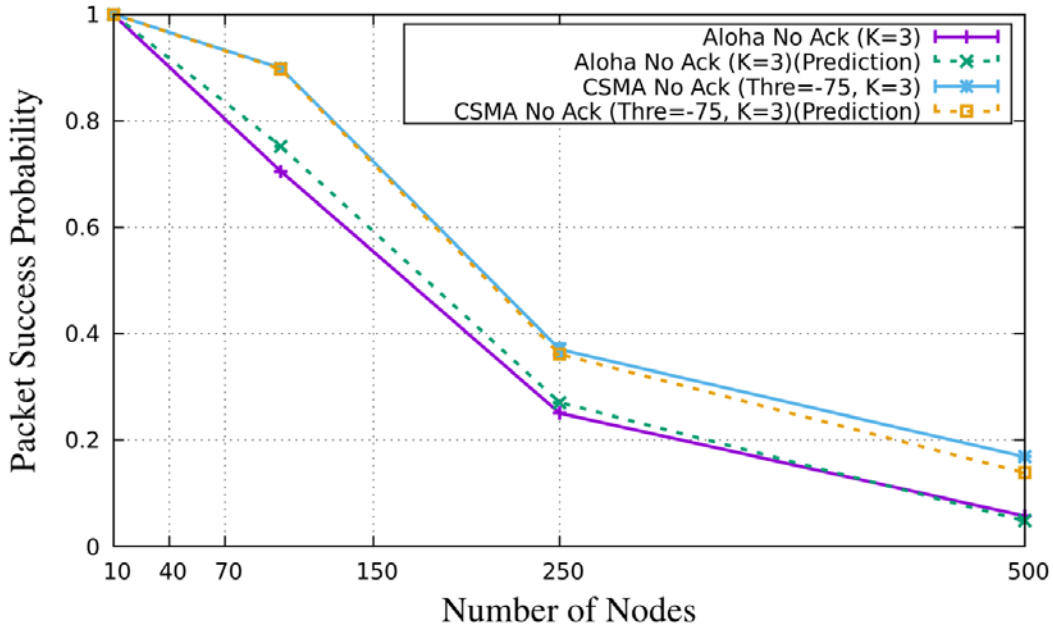


Figure 6.7 : Simulation results vs CNN prediction results

In a real world implementation, we consider that the machine learning algorithm will be incorporated inside the gateway node. This will make the gateway orchestrate the distribution of MAC configurations per node. The cognitive MAC solution is the result of smart MAC parameters tuning for given network conditions, based on the knowledge we acquired by exploiting the network history with the help of a machine learning algorithm.

6.3 Cognitive MAC results

When the CNN provides the output MAC configurations, we simulate the proposed solution with our ns3 platform. The CNN output consists of a set of tables, where each table represents a possible MAC configuration. The content of each table is represented by identification numbers of nodes supposed to use the MAC configuration represented by the table in question.

At the beginning of a simulation, we set the MAC configuration of all nodes, by using the CNN output tables and add several conditions inside the configuration loop to set the optimal MAC configuration distribution. The rest of the simulation methodology remains the same as in the previous chapters.

We show in this section the simulation results of our cognitive MAC and we compare them to static MAC solutions results. Our method takes into account the richness of the training data set. The more different scenarios it contains, the richer a data set is. We show how training the CNN algorithm with poor and rich data sets leads to different results.

We first train CNN with history data of high dense networks, of 500 nodes, which represents a high dense network. We believe that the enhancement obtained by a machine learning based MAC solution (denoted ML MAC in the following) for a high dense network would reflect superior scalability of our proposed solution with respect to static MAC approaches. Afterward, we apply use our optimization ML based solution for medium dense network to evaluate the network performance enhancement we can reach compared to other MAC protocols.

6.3.1 High-dense Network:

6.3.1.a Training set with two possible MAC configurations

The first training set, using data for a network of 500 nodes, contains two scenarios: Aloha No Ack and CSMA No Ack, with a frame retransmission number set at 3 for both. The data set contains the same scenario in terms of node density and traffic intensity, simulated with different seed values. Once the system is trained and reaches a high accuracy ratio, we use the CNN to obtain the MAC configuration distribution for a new network, of same density.

The machine learning algorithm proposes to use CSMA No Ack for all nodes as a best compromise between PSP and ON time. This result might appear not satisfying intellectually, since it does not include any coexistence of MAC protocols, but we believe that this proves that the CNN learned the behavior of the network successfully since, in this simple scenario, configuring nodes with different MAC protocols would negatively affect both PSP and ON time performance. Although the proposed solution is not the best energy wise, it gives good results in terms of compromise between average of PSP, PSP fairness and ON time results. Figure 6.8 shows the obtained average PSP: we can see that the CSMA No Ack and ML MAC are getting the same PSP result. The average ON time results are shown in Figure 6.9, and the ML MAC gives almost the same results as the CSMA No Ack protocol.

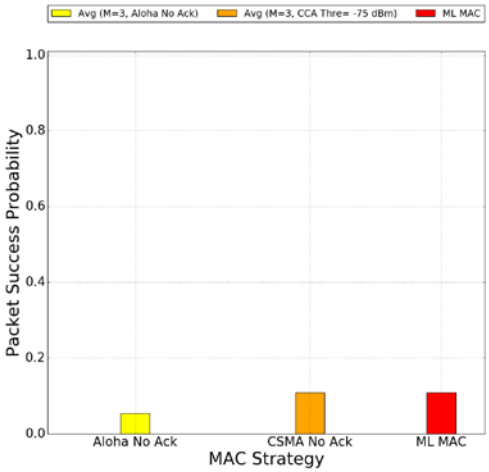


Figure 6.8 : Average PSP results with two possible MAC configurations

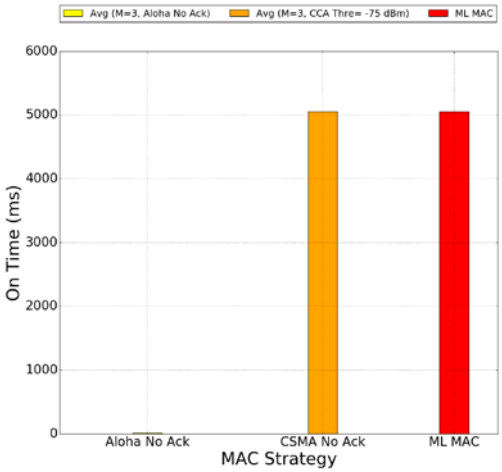


Figure 6.9 : Average ON time results with two possible MAC configurations

6.3.1.b Training set with four possible MAC configurations

Limiting the choice to only two MAC configurations is not very realistic, and it would certainly not require the use of machine learning approaches. Therefore, we continue our study by adding other scenarios to train the CNN algorithm. We introduce Aloha No Ack scenarios with different frame retransmission number, going from 1 to 3. We keep the same single scenario of CSMA No Ack, with K = 3. Now, with a richer training data set in terms of possible configurations, the CNN approach proposes a MAC distribution which can combine these four MAC configurations.

Figure 6.10 shows the PSP result of the proposed cognitive MAC solution and other MAC solutions used in the training data set. We see that the ML MAC outperforms all other MAC protocols. Our proposed solution provides in average 10% better PSP than Aloha No Ack with K = 1, and 20% better PSP than CSMA No Ack with K = 3. These two latter MAC configurations represent respectively the second and the third best average PSP performance.

Figure 6.11 shows the ON time results of our cognitive MAC solution and the remaining MAC solutions. All Aloha No Ack solutions are having very short ON time periods, around tens of milliseconds for each, which represent the frame transmission duration multiplied by the number of retransmissions. The CSMA No Ack is having much longer ON time periods. The proposed cognitive MAC solution consumes in average less than half of CSMA No Ack. Meanwhile, the ML MAC consumes more than Aloha No Ack solutions on average, due to the presence of CSMA nodes. The cognitive MAC is showing a good enhancement in term of trade-off between PSP and ON time, which proves the capacity of the CNN algorithm to exploit the coexistence of MAC protocols without causing performance degradation.

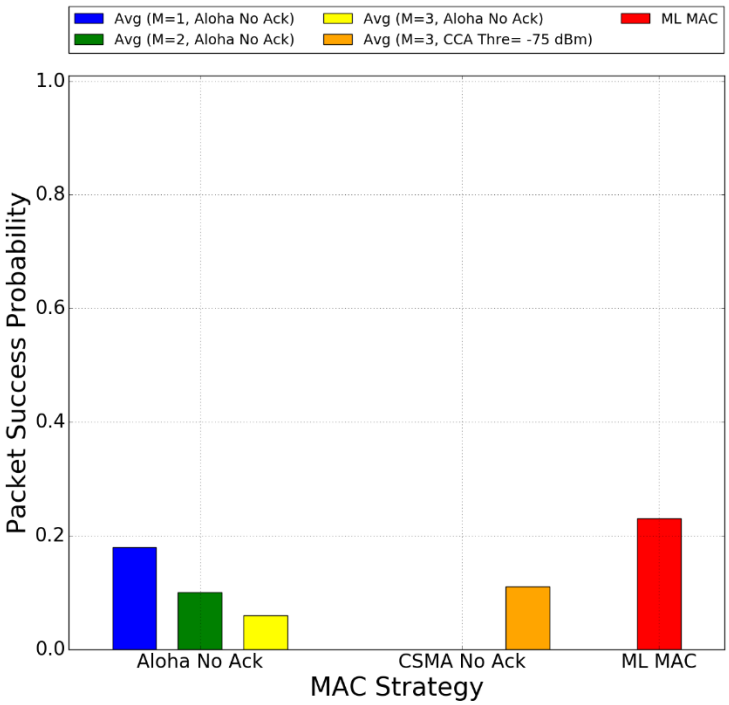


Figure 6.10 : Average PSP results with four possible MAC configurations

With a simple observation of average PSP and ON time results of the MAC configuration present in the data set, we can say that the best compromise is obtained by the Aloha No Ack without frame retransmission, i.e. $K = 1$. However, when we include node fairness results in the discussion (see Figure 6.12), we notice that this latter MAC configuration gives (blue dots) almost binary PSP results, and more than the half of the nodes have zero or near zero PSP result. This feature is not

welcome for IoT network application, especially when almost half of the nodes are practically disconnected.

Our CNN algorithm takes the PSP fairness into account when proposing the cognitive MAC solution, since it tries to improve the performance node-wise, as well as the overall network performance. The CSMA No Ack solution gives the best PSP fairness results with respect to the training static MAC solutions. Our cognitive ML MAC solution gives a better PSP fairness than the CSMA No Ack one: in Figure 6.12 we notice that nodes located between 0 and 40 meters have 10% better PSP than with CSMA No Ack and nodes situated between 40 and 60 meter have better PSP of at least 20% than with CSMA No Ack.

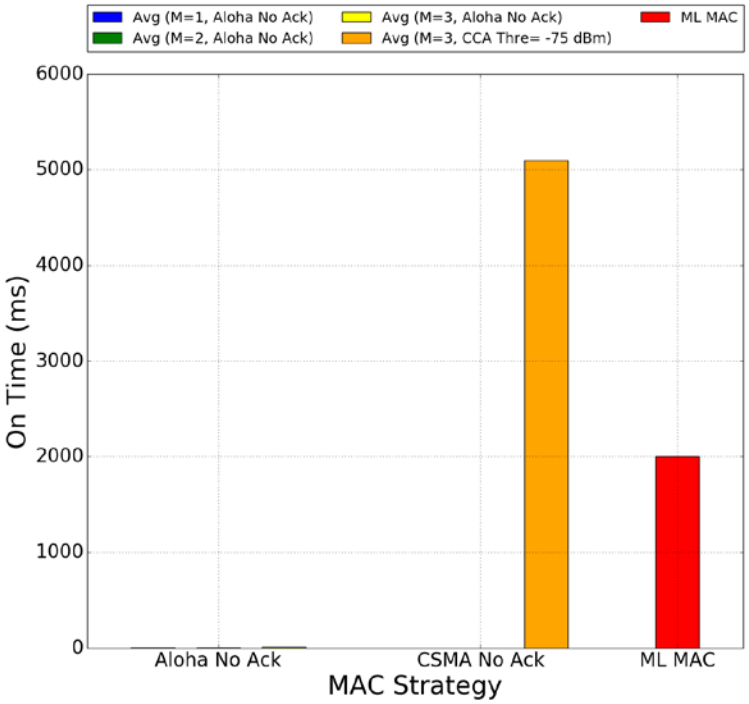


Figure 6.11 : Average ON time results with four possible MAC configurations

The MAC configuration distribution per node is presented in Figure 6.13. In the proposed ML MAC, the nodes that were configured to use Aloha No Ack represent 76% of network nodes. All the Aloha No Ack configured nodes do not use frame retransmission, i.e. $K = 1$. The remaining 24% of the nodes use CSMA No Ack with $K = 3$ as a MAC solution. It is hard to find a correlation between the geographical distribution of the nodes and the choices of the MAC configurations, since some nodes use different MAC configuration while being near one another and having almost the same distance to the gateway node.

One of the reasons of such a distribution could be that the CNN algorithm distributed the MAC configuration in a way to give more fairness of channel access among the node. This directly results in a better PSP fairness and energy efficiency. However, it is interesting to observe that, once the number of possible configurations increases, the ML MAC manages to find a good combination of individual MAC configurations to improve the network performance, demonstrating that MAC protocol coexistence can bring significant benefits. We pursue our analysis in the following, by increasing even more the number of possible configurations.

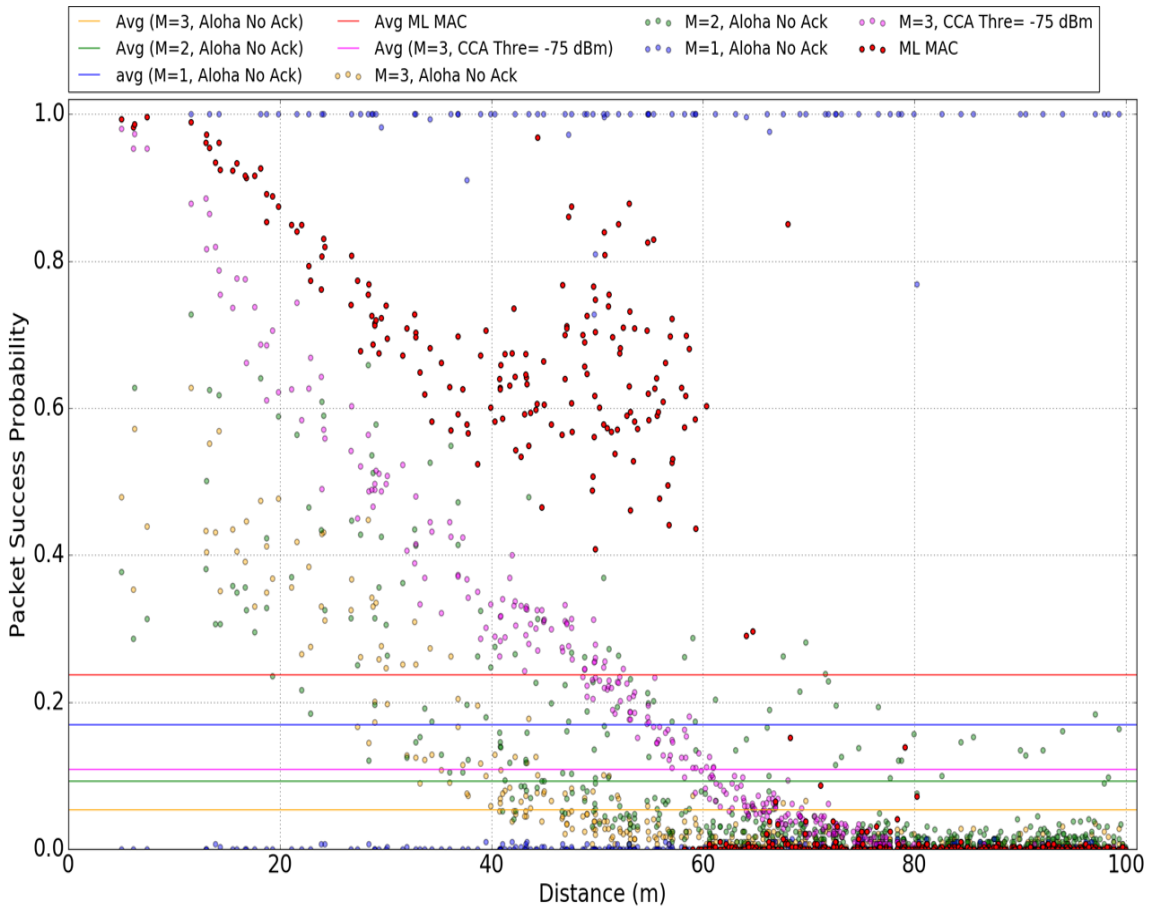


Figure 6.12 : PSP results per nodes with four possible MAC configurations

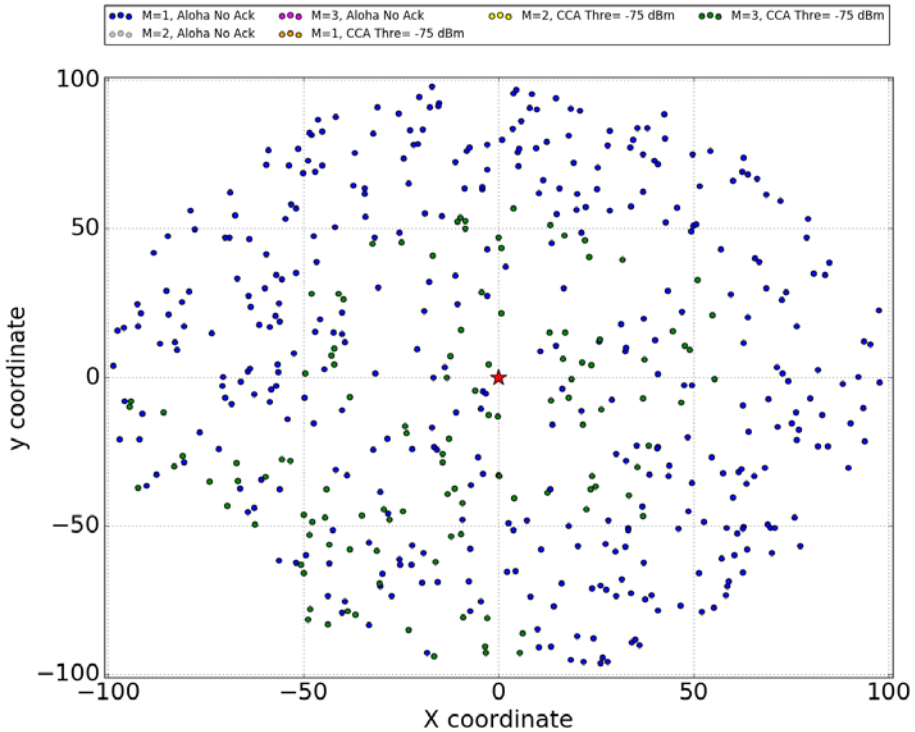


Figure 6.13 : MAC configuration distribution of the ML MAC solution

6.3.1.c Training set with six possible MAC configurations

We continue to enrich the CNN algorithm with new scenarios, we add history data of CSMA No Ack networks with a frame retransmission number set at 1 and at 2. Now, the CNN is trained with networks using six different MAC configurations: Aloha No Ack and CSMA No Ack, with K = 1, 2 or 3. After the training, in the optimization phase, we have a wider choice and the MAC solution can be composed of six different MAC configurations.

Figure 6.14 shows the PSP result of our ML MAC solution and the one of the six static MAC solutions. We see that the proposed cognitive MAC outperforms all other MAC configurations. Our proposed solutions gives a slightly better average PSP than CSMA No Ack with K = 1, 25% better in average than CSMA No Ack with K = 2 and 27% better than Aloha No Ack with K = 1. These two latter MAC configurations represent respectively the second and the third best average PSP performance among the six MAC configurations.

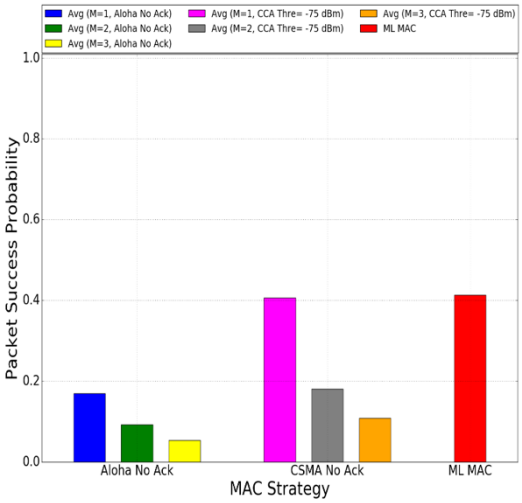


Figure 6.14 : Average PSP results with six possible MAC configurations

Figure 6.15 shows the ON time results of the cognitive ML MAC solution and the one for the static MAC solutions. We first notice that the two CSMA No Ack configurations with K = 2 and K = 3 are the worst energy saving MAC solutions since they have very long ON time periods. The high energy consumption of these solutions, orders of magnitude higher than the other configurations, does not allow a clear visualization of the results. Therefore, in Figure 6.16, we focus only on the best energy saving solutions. We remark that CSMA No Ack with K = 1 is having an acceptable ON time, with an average of 195 ms, which is extremely short comparing to other CSMA No Ack solutions.

The cognitive MAC is then consuming a little more than an Aloha No Ack based network, while ensuring 25% higher PSP than Aloha No Ack with K = 1, which is best Aloha No Ack configuration in terms of PSP and ON time results.

The ML MAC is consuming less energy on average than the half of the CSMA No Ack with K = 1 consumption. When we take into account the ON time fairness, we easily notice that the fairness of our cognitive solution is way better than for the most energy saving CSMA No Ack solution. We remark in Figure 6.16 that, for CSMA No Ack with K = 1, some nodes are consuming a lot more than others, while for the cognitive MAC we have the same ON time periods for most of the nodes. In fact, as discussed below, the ML MAC configures some of the nodes to use Aloha No Ack, with a very short ON time, unnoticeable in Figure 6.16. The remaining nodes, using CSMA No Ack, have very similar activity times.

We can conclude that the CNN algorithm is very efficient in finding a suitable MAC solution. The proposed MAC configuration distribution takes into account the node and the overall network

performance. The CNN algorithm is also able to propose solutions that give the best compromise between PSP and ON time, while taking into account the fairness between network nodes.

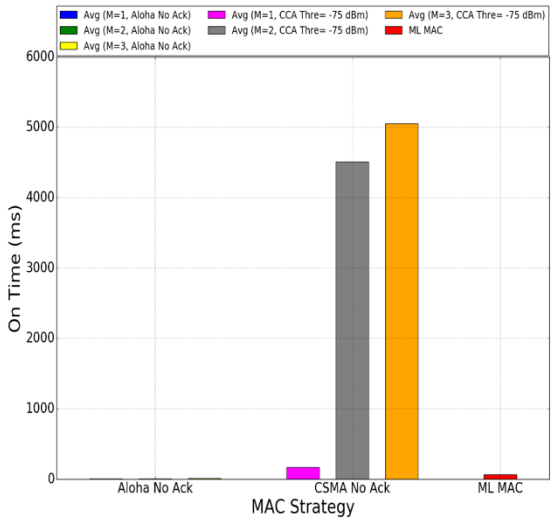


Figure 6.15 : Average ON time results with six possible MAC configurations

As shown in Figure 6.17, for the cognitive MAC, the nodes that were configured to use Aloha No Ack represent 13% of the total. All the Aloha No Ack configured nodes do not use frame retransmission, i.e. they have $K = 1$. The majority of the CSMA No Ack configured nodes do not use frame retransmission either. The remaining 1% nodes use a frame retransmission number of 3, and they are nearest nodes to the gateway. This choice of the CNN algorithm is probably because these nodes are in a critical situation, since their CCA conflict rate is high. More precisely, if they use Aloha No Ack, they will occupy the channel and potentially disrupt the communication of a large number of other devices. If they use CSMA No Ack, they will be discriminated since they are located in a position where they hear all the cell traffic. Hence the CNN algorithm configures them with CSMA No Ack with $K = 3$, to add some redundancy and increase their success probability.

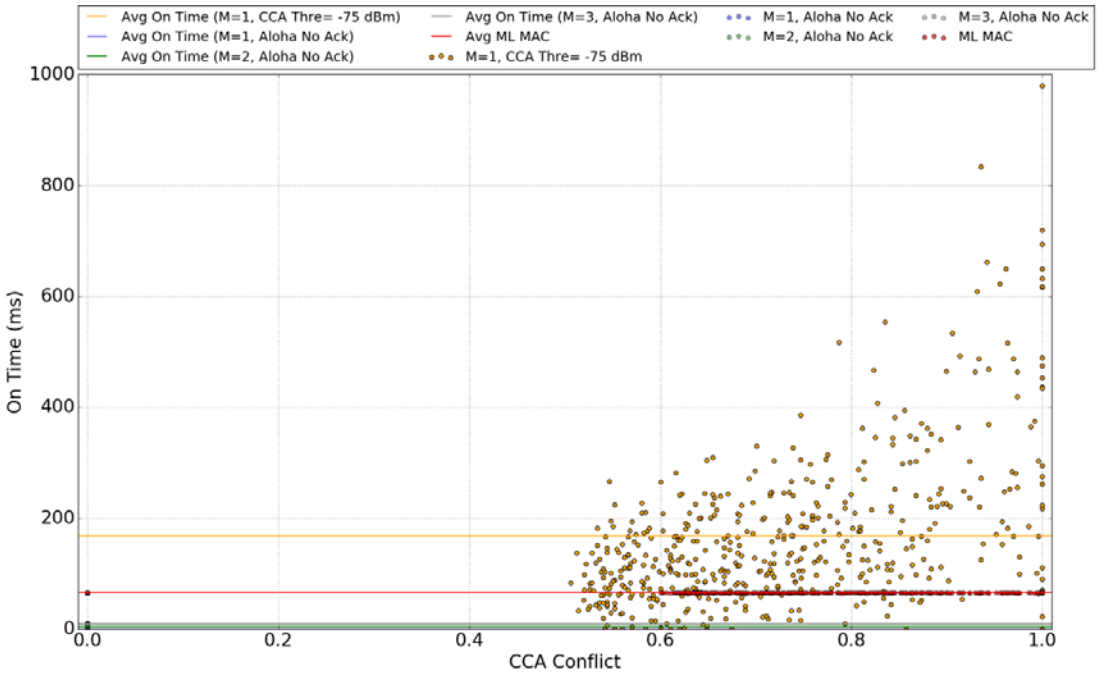


Figure 6.16 : ON time results for ML MAC vs. static MAC configurations

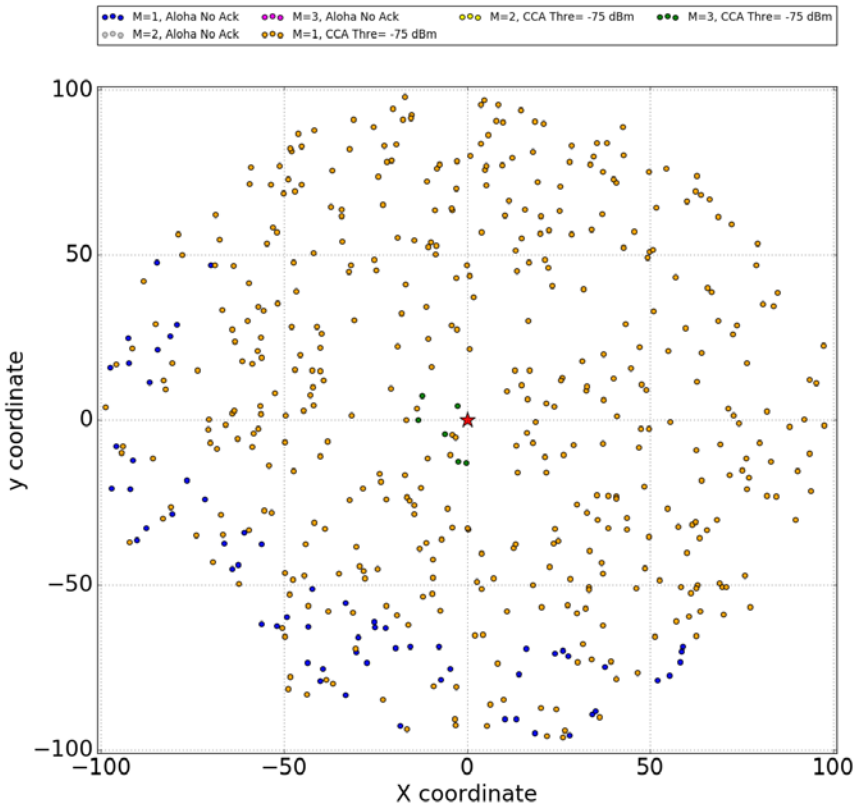


Figure 6.17 : MAC configuration distribution of the Cognitive MAC solution

6.3.2 Medium-dense Network:

In the previous section, we showed how the use of CNN algorithm and allowing the coexistence of different MAC configuration can bring benefits for a high-dense network. We can say that, for a loaded network condition, the enhancement obtained with our cognitive MAC reflect a promise of a better scalability for LPWAN. In this high load scenario, ML MAC manages to increase the PSP up to 40%, but this is still a low value, as the network is highly overloaded. Such a scenario is unlikely in practice, since it indicates a poor infrastructure deployment.
Therefore, in this section we consider a medium-dense network (250 nodes with our simulation settings), where the obtained results with static MAC approaches are already satisfying. The goal here is to measure the gain we can obtain by adding cognition capacities to the MAC layer in these more realistic conditions.
Figure 6.18 shows the PSP results of all MAC configurations and the PSP obtained by the ML MAC solution. We can see that CSMA No Ack with K = 1 is giving by far the highest PSP result among the static solutions, with around 50% better PSP than an Aloha No Ack with K = 3 configuration, and 35% better than CSMA No Ack with K = 3.
Figure 6.19 shows the ON time results of all MAC configurations. Once again, it is obvious that the two MAC configurations CSMA No Ack with K = 2 and K = 3 are giving the longest activity time periods and rendering the visualization of the other results difficult. Hence, in Figure 6.20 we show the individual ON time results only for the best energy saving MAC protocols. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC configuration also have perfect ON time fairness results, where all the nodes are getting the same ON time period.

CSMA No Ack with K = 1 is the best CSMA based protocol in terms of energy efficiency; it gets an ON time average period of nearly 70 ms and a range of values that goes from a few milliseconds to 300 ms.

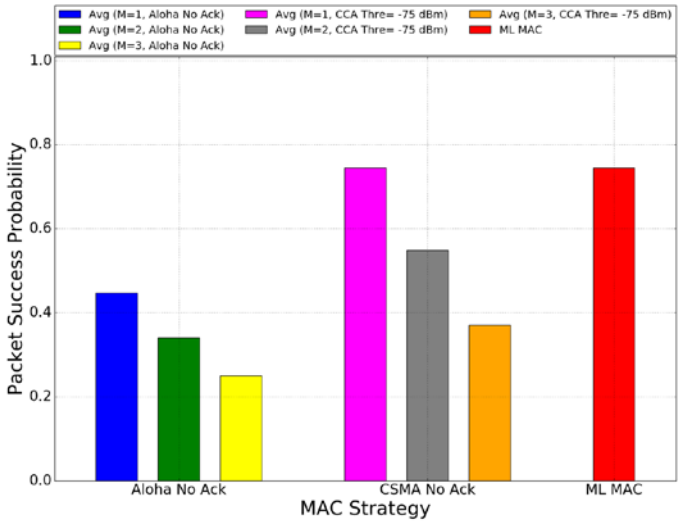


Figure 6.18 : PSP results with six possible configurations in medium-dense network

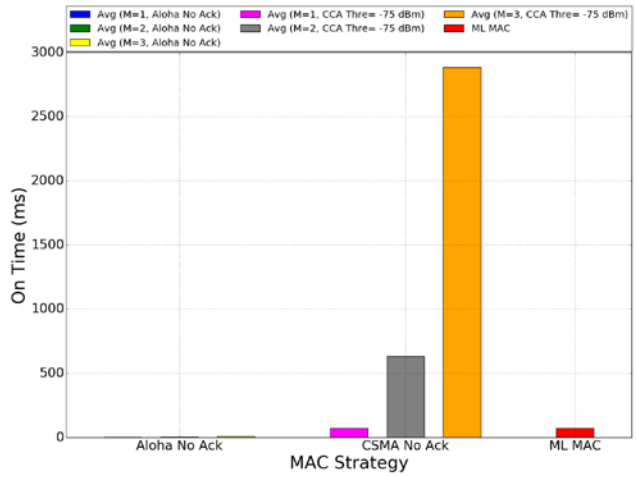


Figure 6.19 : ON time results with six possible configurations in medium-dense network

The cognitive ML MAC proposed by the CNN algorithm, for this network density and traffic intensity, is simply to use the CSMA No Ack with K = 1 for all nodes, since it is the MAC configuration distribution that gives the best compromise between PSP, ON time and fairness results.

Since the choice was easy to make, due to the clear superiority of CSMA No Ack with K = 1, we prefer now to imagine a scenario where this configuration is not available to use. Then, we force the CNN not to choose the CSMA No Ack with K = 1 at all, in order to see if the ML algorithm is capable to propose a proper solution when several close configurations are available.

Figure 6.21 shows the PSP results of all MAC configurations except CSMA No Ack with K = 1, and the PSP obtained by the ML MAC solution. We can see that the ML MAC is giving the highest PSP result, with 33% better PSP than an Aloha No Ack with K = 3 MAC configuration and 22% better than CSMA No Ack with K = 3. The ML solution is close to the CSMA No Ack with K = 2 MAC configuration (only 3% in terms of average PSP), but is gives a much better performance in terms of activity time.

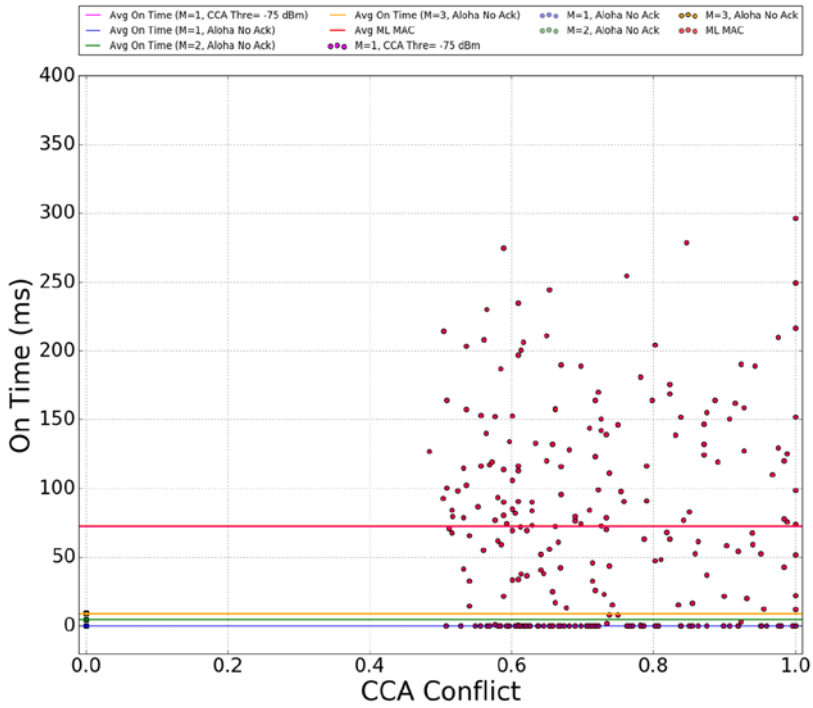


Figure 6.20 : ON time results of ML MAC for a medium-dense network

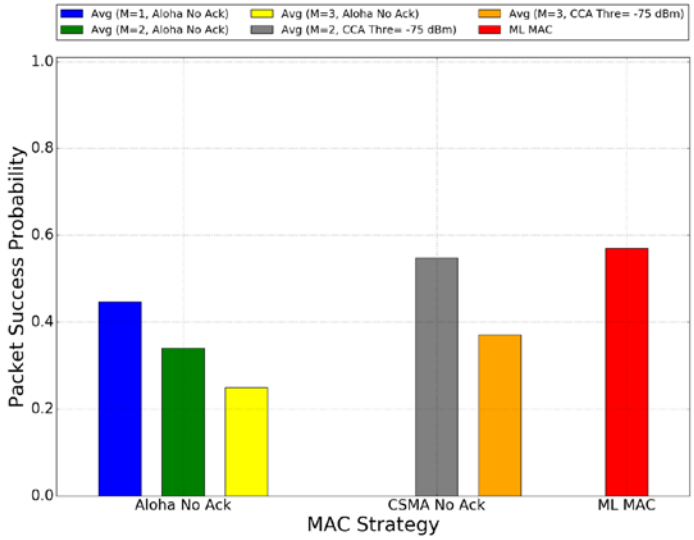


Figure 6.21 : PSP results for ML MAC without CSMA No Ack with K=1

Indeed, Figure 6.22 shows the ON time results when the CSMA No Ack with $K = 1$ configuration is not available. CSMA No Ack with $K = 2$ is now the best CSMA-based protocol in term of energy efficiency: it has an ON time average period of nearly 600 ms and a range of values (see Figure 6.23) that goes from 250 ms to near 1900 ms. The ML MAC ON time results represent the good compromise between Aloha based MAC configurations and the increased PSP brought by CSMA based MAC. The cognitive ML MAC provides an average ON time period of 125 ms, which is almost five time less than CSMA No Ack with $K = 2$, and shows a good ON time fairness result, as depicted in Figure 6.23.

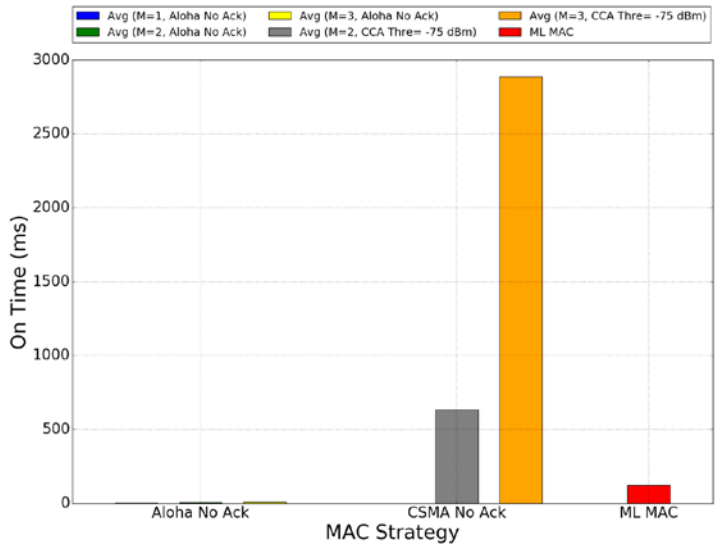


Figure 6.22 : ON time results for ML MAC without CSMA No Ack with K=1

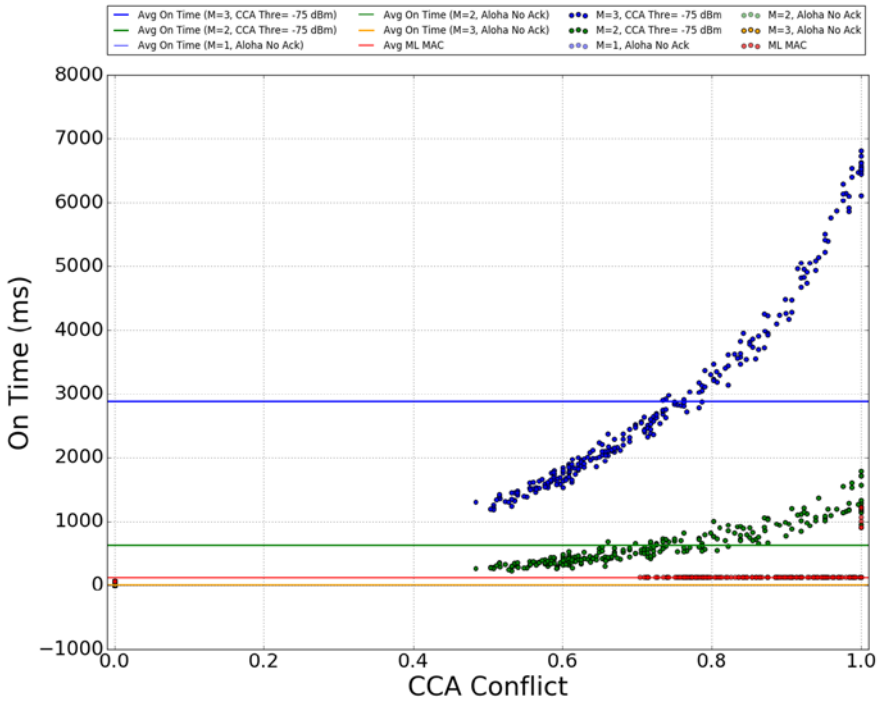


Figure 6.23 : Individual ON time results for ML MAC without CSMA No Ack with K=1

Figure 6.24 shows the MAC configuration distribution for the cognitive ML MAC solution among the nodes of the cell. We see that the majority of the nodes are configured with Aloha No Ack with $K = 1$ and with CSMA No Ack with $K = 2$, with the exception of 5 nodes that are the nearest to the gateway and use CSMA No Ack with $K = 3$. The nodes that use Aloha No Ack with $K = 1$ represent 40% of the nodes and are those situated the furthest to the central sink node. The nodes that use CSMA No Ack with $K = 2$ represent around 58% of the nodes and are situated in the middle region of the cell.

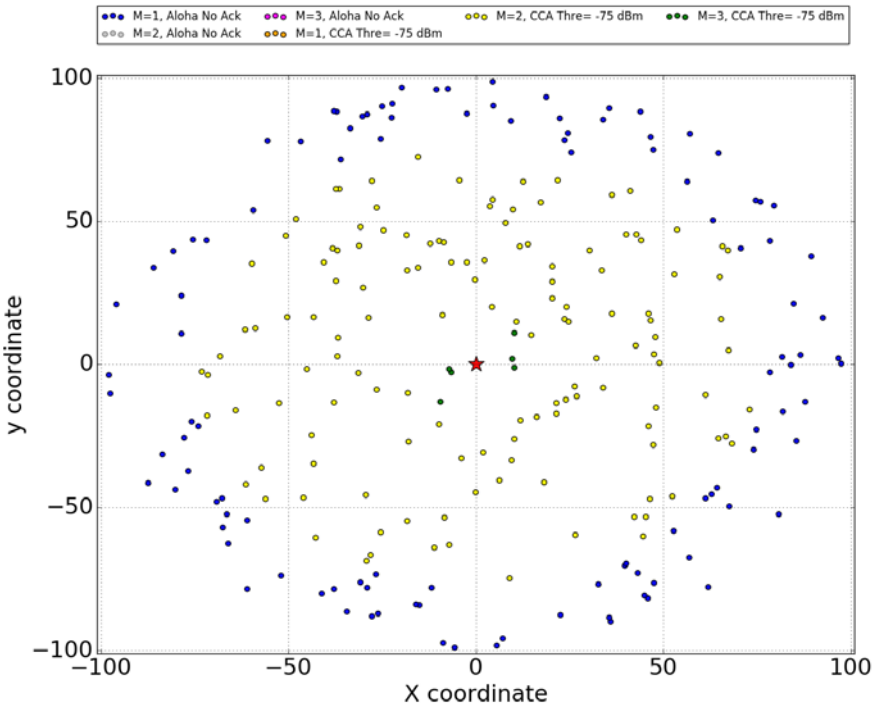


Figure 6.24 : MAC configuration distribution of the Cognitive MAC solution

The choice made by the CNN offers 50% higher PSP than Aloha No Ack with K = 3. This latter MAC configuration, as discussed in previous chapters, is pretty similar to the MAC solution used by SigFox. We believe that offering such an enhancement, of 50%, for medium-dense networks, with a reasonable supplementary energy consumption, is a very promising result that encourage the use of ML based MAC solution for dedicated IoT network. We show inhere that we can achieve an interesting reliability improvement without frequency diversity, but only by allowing the coexistence of different MAC configurations.

6.4 Conclusion

In this chapter, we presented our machine learning based MAC solution for dedicated IoT networks. We showed how our proposed solution is capable of taking advantage of both classic MAC approaches, Aloha and CSMA, by allowing their coexistence within the same cell. Our solution takes into consideration the transmission reliability, the energy consumption and the fairness between the cell nodes. This contribution is the fruit of the analysis we conducted in previous chapters, which allowed us to identify key parameters that need to be tuned dynamically in order to give the best network performance.

We gradually exposed the CNN algorithm to an increased number of possible configurations and to different network densities. Our results show that, when one MAC configuration outperforms the others, the ML MAC is able to pick it and converge to it. However, the ML MAC is mostly interesting in scenarios where several MAC configurations give similar results. In this case, a cognitive MAC approach is able to find the perfect distribution of MAC configurations, which is not always obvious, even for a human expert.

We showed through extensive simulation the enhancement in terms of packet success probability and activity time period that could be obtained with a machine learning based MAC. For a loaded network, the PSP gain obtained by the ML MAC with respect to static MAC configuration reflect a

promise of a better scalability for dedicated IoT networks. To the best of our knowledge, this is the first work that proposes a cognitive MAC solution for dedicated IoT networks.

7. Machine Learning MAC in Heterogeneous Deployments

In the previous chapter, we proved the interest of a machine learning algorithm, based on CNN, to predict the network performance and to adapt the MAC layer configuration to the network situation. The solution obtained by CNN is a combination of different MAC configurations, belonging to different MAC protocols. The simulation results showed the superiority of our cognitive strategy in terms of packet success probability, activity time and fairness between the cell nodes.

Through this chapter, we add more realistic conditions to our machine learning algorithm and to the simulation setup. We start by removing the distance to gateway information from the input data of the CNN algorithm, as this parameter is difficult to measure in practice. We replace this information by the node activity time. Based on the analysis conducted in Chapter 5, we believe that the node activity time contains an indication about the distance separating the node and the gateway, and it is directly measurable by the node itself.

The second, and most significant modification in this chapter is that we change the uniform node distribution in the cell, in order to have more heterogeneity in terms of traffic, channel quality and interference inside the cell. We consider that nodes in an IoT network will often be deployed around hotspots, very different from a uniform deployment. Adding more realistic conditions helps us to investigate the feasibility of implementing our machine-learning-based MAC solution in a real LPWAN cell.

7.1 Input data adaptation

In this section modify the input data for the machine-learning algorithm to be closer to a real implementation of the cognitive MAC solution. We believe that the distance to the gateway is hard to obtain with a good accuracy in a real LPWAN network; we therefore propose to use another metric in the training process instead, the node activity time.

We remind that the node activity time is the time that a node spends with its radio turned on. For the case of an Aloha No Ack node, it would be the time that the node takes to send the frame on the radio. Meanwhile, for a CSMA No Ack node, we add to that the time spend to sense the channel and the waiting back-off time until the node obtains access to the channel. We consider that each node is able to measure its activity time and, for a real implementation, the nodes will be supposed to send this information to the gateway periodically.

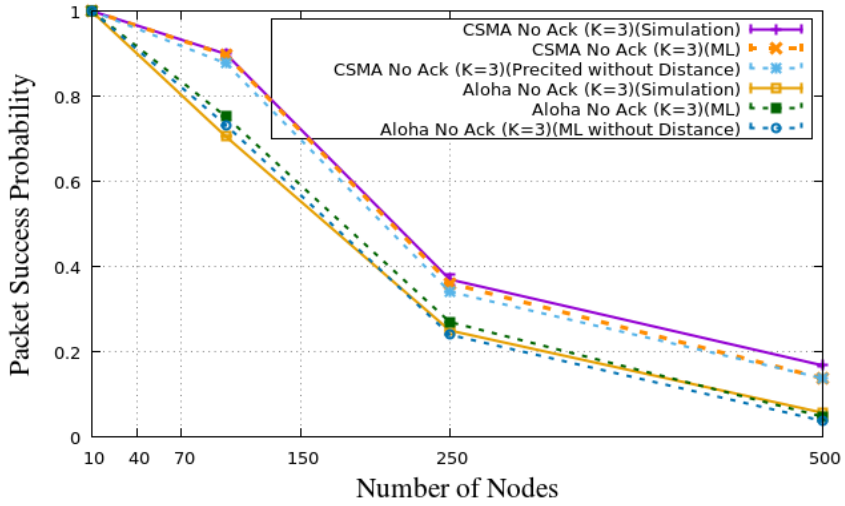


Figure 7.1 : CNN prediction results with activity time as input data

Hence, we trained the CNN algorithm with the new input data set. Figure 7.1 shows the CNN predicted results in terms of PSP and simulation results for the Aloha No Ack and the CSMA No Ack protocols, and for different network densities, going from low dense network to high dense network. The simulation results are shown with confidence interval of 95% and the prediction results are average values over 10 predicted results. Figure 7.1 shows that the predicted PSP values are pretty similar to the simulated results, which validates the accuracy of our CNN model.

The CNN algorithm with this new input data set is used for the same machine-learning approach previously explained, in order to predict the optimal MAC configuration for different network situations, but for heterogeneous deployments.

7.2 Heterogeneous nodes distributions

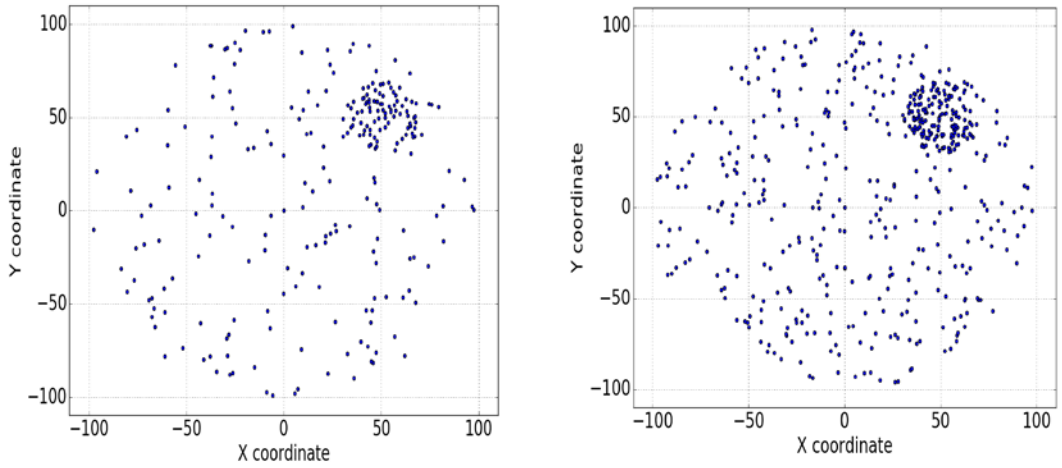
We continue throughout this section to add realistic conditions to the CNN based MAC solution. It is clear that, in a real dedicated IoT cell, there will be areas denser than others inside the gateway coverage zone. This would result in heterogeneous traffic, interference and channel quality inside the cell. We believe that the cognitive MAC solution is the correct way to manage the channel sharing in such a context, since static protocols, or even classical adaptation mechanisms (*e.g.* binary exponential back-off), have difficulties in such heterogeneous conditions, as we will prove throughout this chapter.

Therefore, we include non-uniform node distributions to our study, with the focus on two heterogeneous distributions: cells with one dense region and cells with two dense regions. In the first distribution, with one dense region, we studied two possibilities: a cell with one dense region containing the third of the cell nodes, while the rest of the cell contains scattered nodes, and a cell with one dense region containing half of the cell nodes. These two deployment distributions are denoted, respectively, one third region and one half region, in the following.

Meanwhile, for the deployment with two dense regions, the nodes are distributed as follows: one region in the cell that contains the third of cell nodes, a second region that contains the half of the cell nodes, and the remainder of the cell contains scattered nodes.

7.2.1 One third region

We inhere focus on the one third region distribution. We include the same node densities as in the previous chapter, 250 and 500 nodes, which respectively represent a medium-dense and a high-dense network.



(a) 250 *(b) 500*

Figure 7.2 : One third dense region for networks of 250 and 500 nodes

Figure 7.2 shows the nodes repartition in the cell, for 250 and 500 nodes networks. The dense region is represented by the darker circle shaped region, located in the top right of each sub-figure. We used our simulator to run all the MAC configurations, previously presented in Chapter 6, for this type of node distribution. Afterward, the simulation results were used to train the CNN algorithm. We then exploit our machine-learning solution to get the MAC configuration for a such heterogeneous node distribution.

7.2.1.a High-dense network

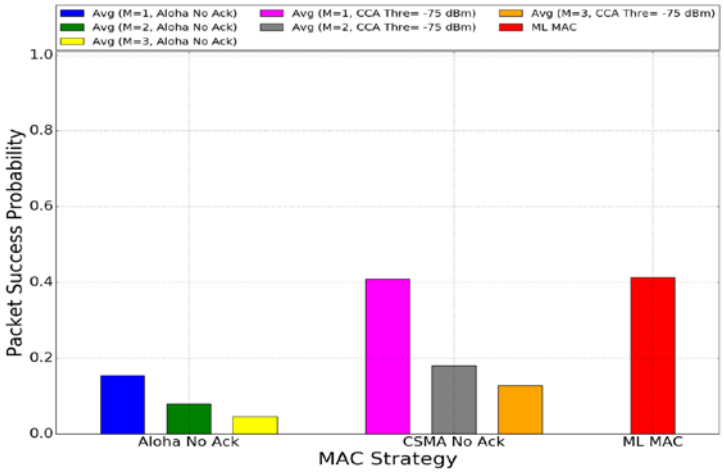


Figure 7.3 : PSP results for ML MAC in a high-dense network

Figure 7.3 shows the average PSP results of all static MAC configurations and the PSP obtained by the ML MAC solution. We can see that the ML MAC is giving the highest PSP result, with 37% better PSP than an Aloha No Ack configuration with $K = 3$, and 25% better than CSMA No Ack with $K = 3$. The best static configuration is CSMA No Ack with $K = 1$, and the ML solution slightly outperforms it, bringing a small gain in terms of PSP.

In Figure 7.6, we show the PSP results per node, in function of the distance between the node and the gateway node. We show only results for the best static CSMA No Ack, the best static Aloha No Ack and the ML MAC configuration. We can see that CSMA No Ack with $K = 1$ is better in terms of PSP fairness than Aloha No Ack with $K = 1$. The latter protocol has almost binary PSP results, close to either 1 or 0, while CSMA No Ack has a much lower number of nodes with a PSP close to 0. The ML MAC solution has the lowest number of nodes with a PSP less than 1%, and keeps almost the same PSP fairness result as those of CSMA No Ack with $K = 1$.

Figure 7.4 shows the average ON time results of all MAC configurations. It is obvious that, as in the previous chapter, the two CSMA No Ack MAC configurations with $K = 2$ and $K = 3$ are giving the longest activity time periods. In Figure 7.5, we show the ON time results per node, showing the best energy saving protocols in function of the distance. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC configurations are also giving a perfect On Time fairness result, since all the nodes are getting the same ON time period. As explained before, that is thanks to the absence of any carrier sense mechanism when Aloha is used at the MAC level.

CSMA No Ack with $K = 1$ is the best CSMA based protocol in terms of energy efficiency. It gets an ON time average period of nearly 200 ms and a range of values that goes from a few milliseconds to hundreds of milliseconds. When CSMA No Ack is used without any frame retransmission ($K = 1$), the back-off window stays at its minimum value, hence the node does not wait for a long number of slots before sending. This is what explains the reasonable ON time results of this MAC configuration.

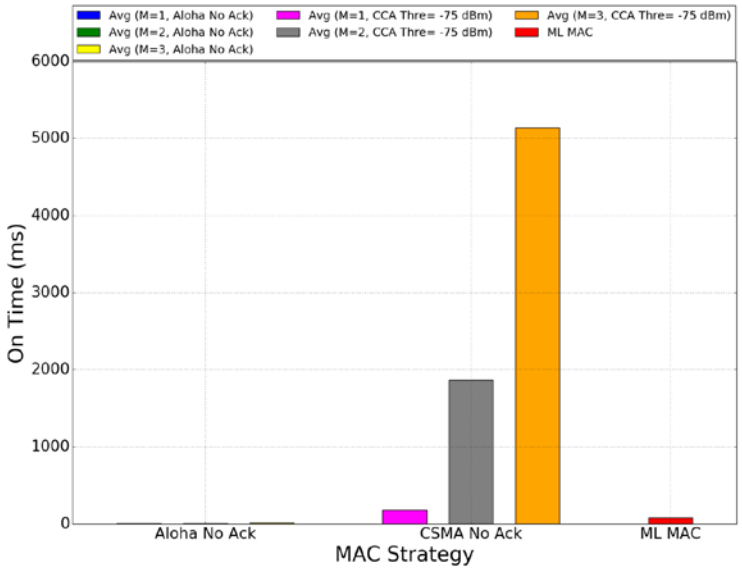


Figure 7.4 : ON time results for ML MAC in a high-dense network

The cognitive ML MAC ON time results represent a good compromise between Aloha based MAC configurations and the best CSMA based MAC. The cognitive MAC provides an average ON time period of 70 ms, which is less than half the one obtained by the CSMA No Ack with K = 1, and shows a good ON time fairness. Just like in Aloha based solutions, most of the nodes have a similar activity time, close to the average values. However, unlike in Aloha No Ack, a few nodes, unnoticeable in the figure, have a much higher ON time. This can seem unfair for these nodes, but one can also argue that, if this phenomenon concerns a limited number of nodes, it would not be difficult to equip these nodes with special batteries, a price to pay in order to create a perfect energy fairness for the other nodes.

Figure 7.7 shows the MAC configuration distribution for the cognitive ML MAC solution, depicting all the nodes of the cell. We see that the majority of the nodes, 86% of them, are configured to use a CSMA No Ack without any frame retransmission (K = 1). The rest of the nodes are all configured to use Aloha No Ack with K = 1, with the exception of two nodes that are configured to

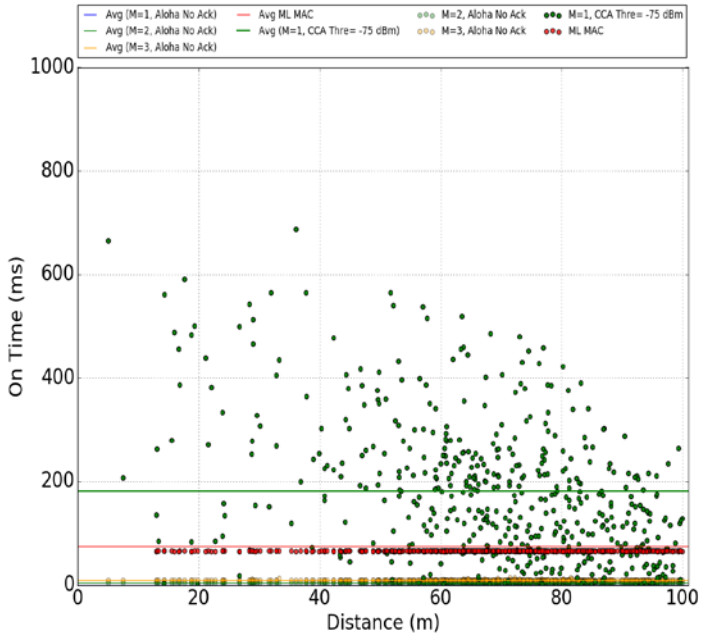


Figure 7.5 : Individual ON time results in one third region deployment

use CSMA No Ack with $K = 3$ as a MAC solution. This exception is given for two nodes that are the closest to the gateway, since they are then able to hear all the traffic of the cell. The ML algorithm chose $K = 3$ for these two nodes in order to boost their chance to access the channel, since their CCA mechanism would return busy very often. Meanwhile, if we configure these two nodes with an Aloha-based MAC, then they will block all other nodes from reaching the gateway.

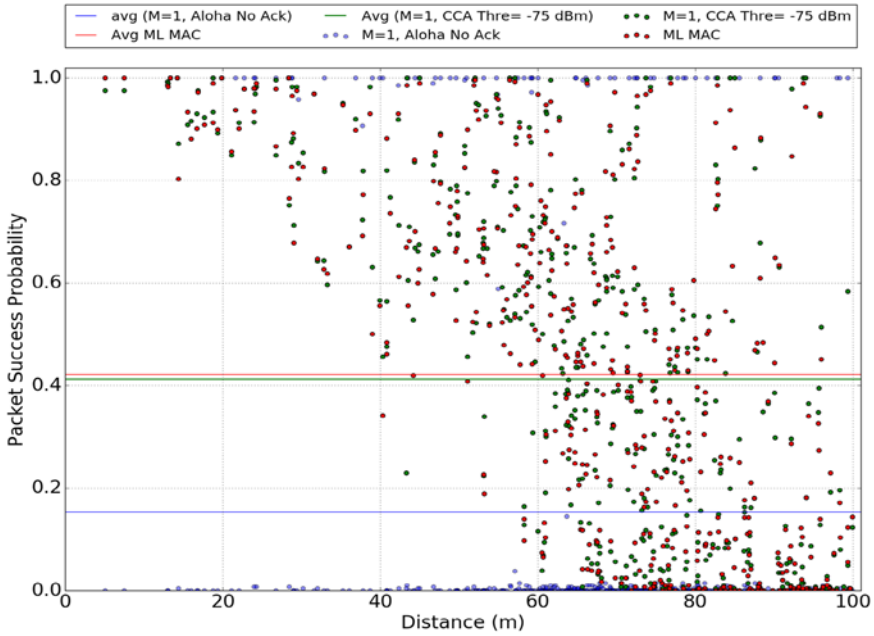


Figure 7.6 : Individual PSP results in one third region deployment

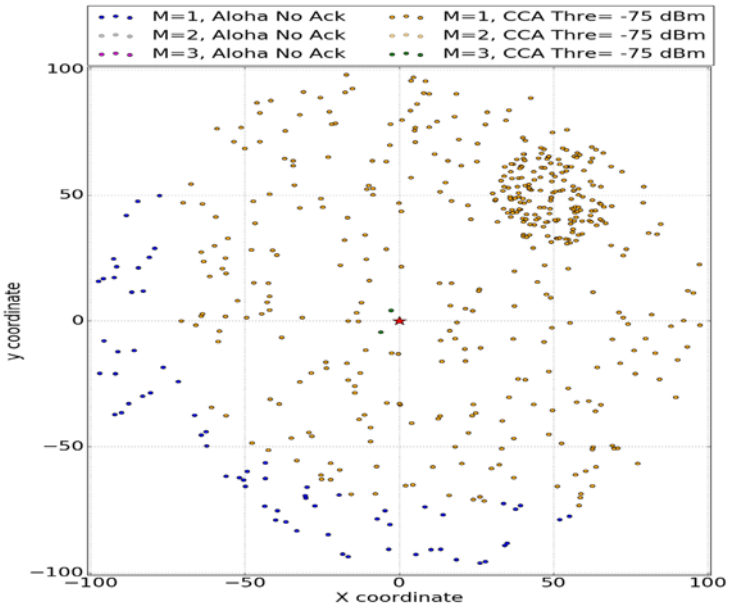


Figure 7.7 : MAC configuration for ML MAC in a high dense one third region

7.2.1.b Medium-dense network

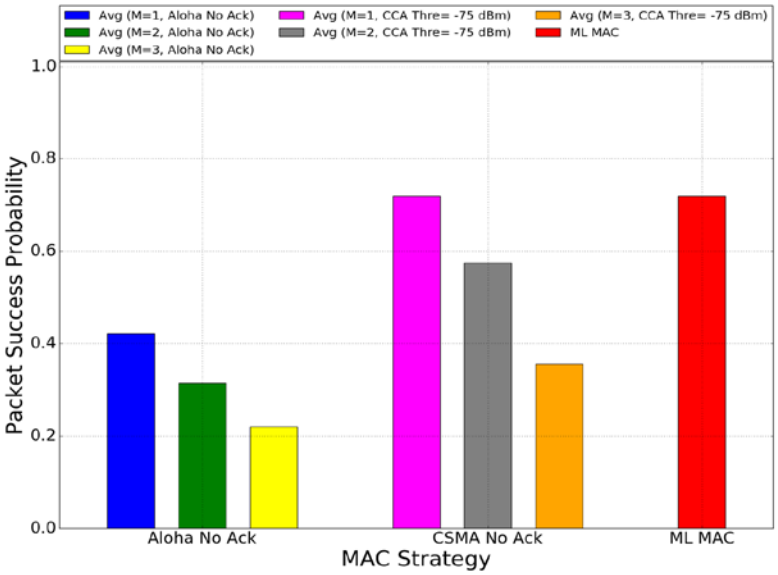


Figure 7.8 : PSP results for ML MAC in a medium-dense network

Figure 7.8 shows the average PSP results of all MAC configurations and the PSP obtained by the ML MAC solution for a medium-dense network. We can see that the CSMA No Ack with $K = 1$ is giving the highest PSP result, with almost 50% better PSP than Aloha No Ack with $K = 3$, and almost 30% better than CSMA No Ack with $K = 3$.

Figure 7.9 shows the average ON time results of all MAC configurations. It is obvious that the two CSMA No Ack configurations with $K = 2$ and $K = 3$ are giving the longest activity time periods. In Figure 7.10 we show the ON time results per node, only for the remaining protocols, that represent the most energy saving MAC configurations. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC configurations are having perfect ON time fairness results, since all the nodes are getting the same ON time period.

As in the other scenarios, CSMA No Ack with $K = 1$ is the best CSMA based protocol in term of energy efficiency. It gets an ON time average period of nearly 30 ms and a range of values that goes from a few milliseconds to 200 ms. For CSMA No Ack with $K = 1$, we have 54% of the nodes getting an ON time shorter than 10 ms, 42% that reach an activity time of less than 100 ms, and only 4% with an ON time longer than 100 ms.

The decision of the cognitive ML MAC based on the CNN, for this network density and node distribution, is simply to use the CSMA No Ack with $K = 1$ for all nodes, since it is the MAC configuration distribution that gives the best compromise between PSP, ON time and fairness results. The choice is simple to make in this case, due to the superiority of performance of CSMA No Ack with $K = 1$ with respect to other MAC configurations in terms of PSP and ON time, for average results on the entire networks, but as well as local node performance.

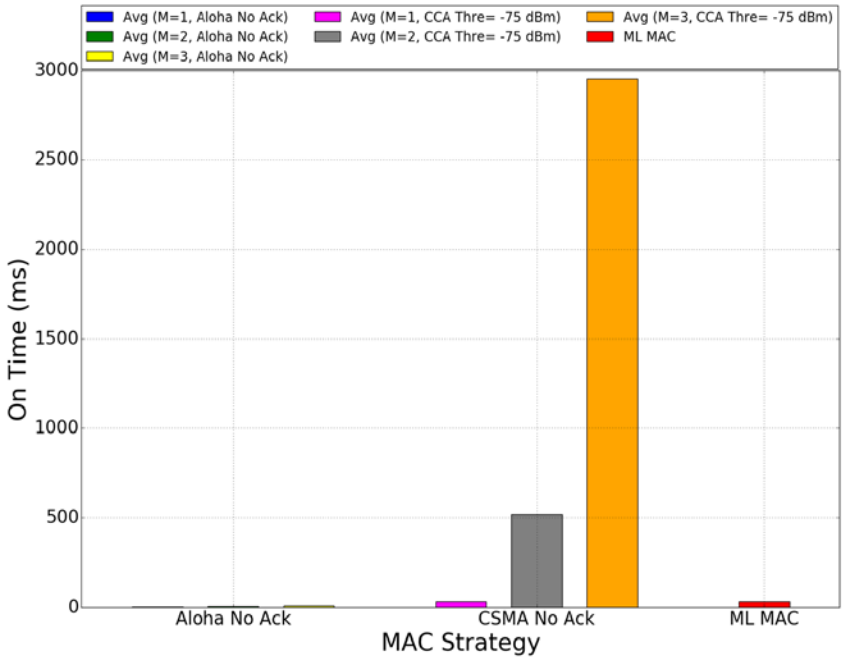


Figure 7.9 : ON time results for ML MAC in a medium-dense network

Similarly, to Chapter 6, we wanted to add more complexity to our scenario, by forcing the CNN not to choose the CSMA No Ack with $K = 1$. The goal here is to use the CNN algorithm without having a simple choice to make between configurations, as in the previous case.

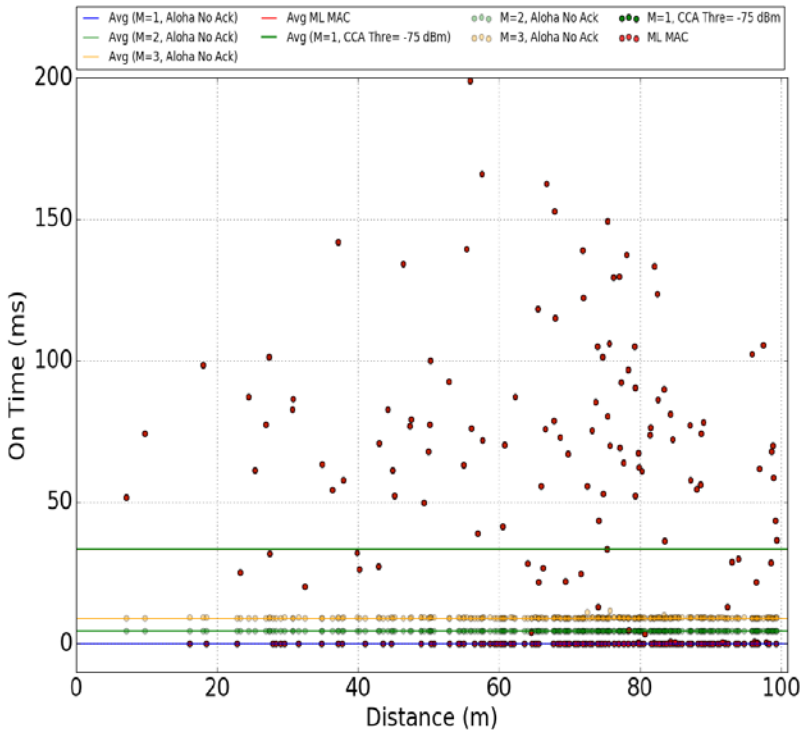


Figure 7.10 : Individual ON time results for a medium-dense network

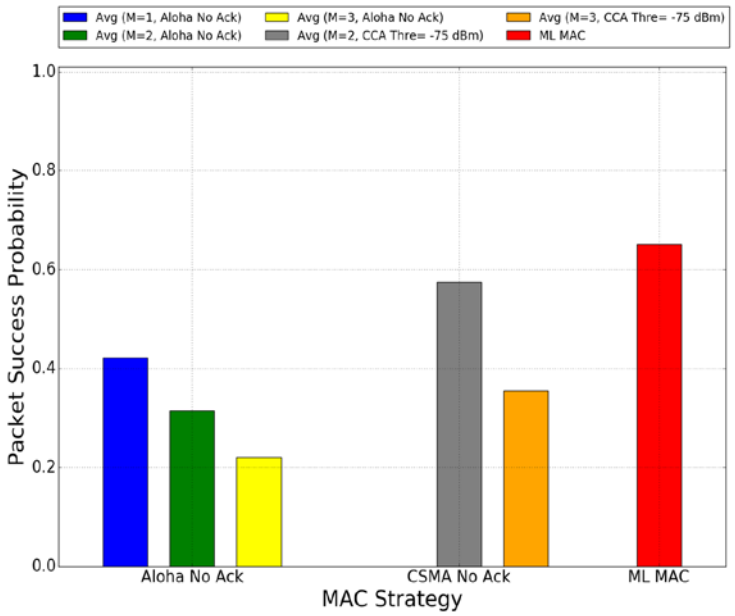


Figure 7.11 : PSP results for ML MAC without CSMA No Ack with K=1

Figure 7.11 shows the average PSP results for ML MAC and for all the static MAC configurations, except for CSMA No Ack with K = 1. We can see that the ML MAC is giving the highest PSP result, with 43% better than an Aloha No Ack configuration with K = 3, and 27% better than CSMA No Ack with K = 3. The ML MAC solution outperforms the CSMA No Ack configuration with K = 2 by 10%, also giving better PSP fairness results, as we can notice in Figure 7.13.

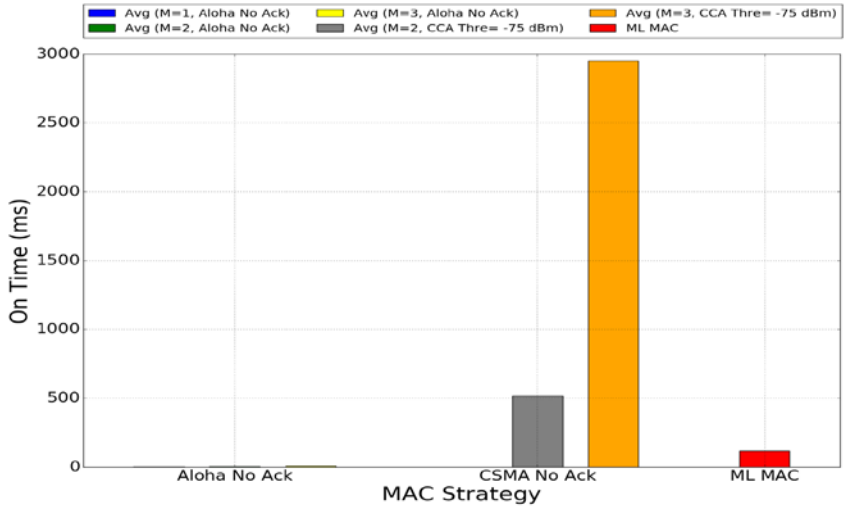


Figure 7.12 : ON time results for ML MAC without CSMA No Ack with K=1

Figure 7.12 shows the average ON time results of all MAC configurations, except for CSMA No Ack with K = 1. CSMA No Ack with K = 2 is now the best CSMA based protocol in terms of energy efficiency: it has an average ON time period of nearly 500 ms and a range of value that goes from 100 ms to 1000 ms. The cognitive MAC ON time results represent the good compromise between Aloha based MAC configurations and the best CSMA based MAC. The cognitive MAC provides an average ON time period of 116 ms, which is almost five time less than the one of CSMA No Ack with K = 2 and shows a good ON time fairness results.

Figure 7.14 shows the MAC configuration distribution of the cognitive ML MAC solution among the nodes of the cell. We see that the majority of the nodes, 78% of them, are configured at the MAC layer level to use CSMA No Ack with K = 2. The rest of the nodes are all configured to use

Aloha No Ack with K = 1. The nodes that use Aloha No Ack with K = 1 are in their majority the nodes farthest away from the dense region, except for a few nodes that are very close to the dense region but whose PSP and ON time performance cannot be enhanced with a carrier sense mechanism, due to their position and CCA conflict rate.

This latter result shows the power of the machine learning algorithm to combine different MAC configurations in order to offer the best network performance results. We believe that only a machine learning based solution could make of protocol coexistence a strength for the network.

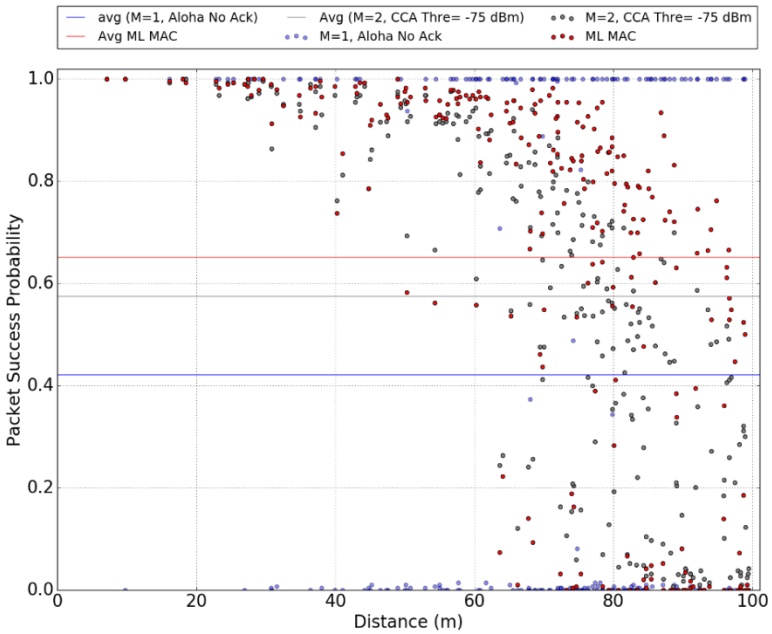


Figure 7.13 : Individual PSP results for ML MAC without CSMA No Ack with K=1

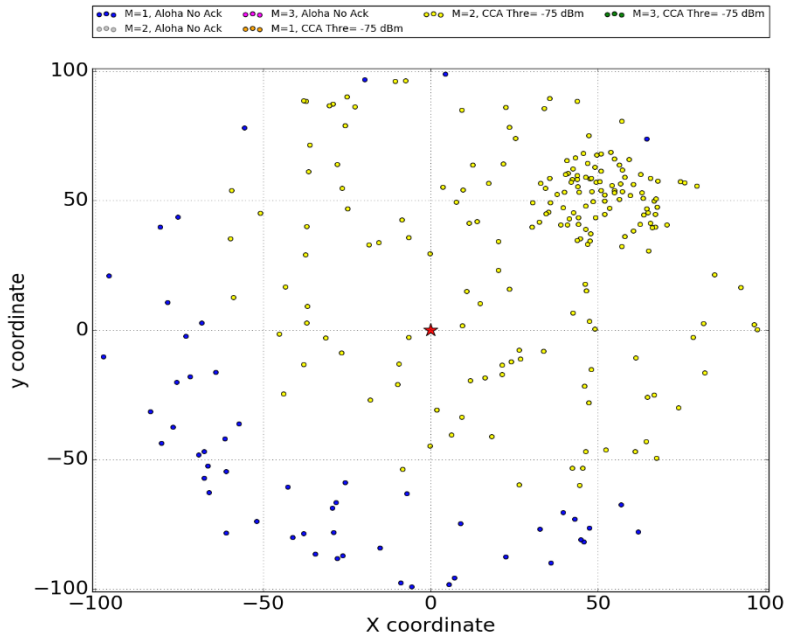
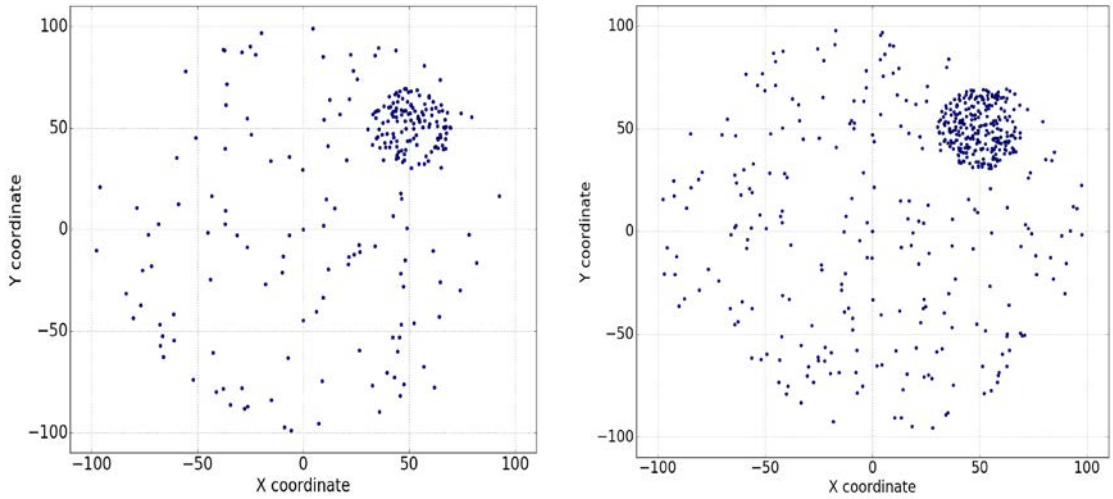


Figure 7.14 : ML MAC configuration distribution without CSMA No Ack with K=1

7.2.2 One half region

We apply here the same non uniform distribution as in the previous section, but we increase the density inside the dense region: we now have half of the nodes concentrated in a dense region and the other half scattered in the cell. We believe that this scenario is also more realistic than with a uniform node distribution. Figure 7.15 shows the node distribution used in this section, for both medium-dense and high dense networks.

We used ns3 simulation to study the performance of all MAC configurations for such node distribution. Then, the simulation data were used to train the CNN in order to predict and provide the optimal MAC solution for such network condition.



(a) 250 Nodes *(b) 500 Nodes*

Figure 7.15 : One third dense region for networks of 250 and 500 nodes

7.2.2.a High-dense network

Figure 7.16 shows the average PSP results for all static MAC configurations and the PSP obtained by the cognitive ML MAC solution. The cognitive MAC solution is having the best PSP

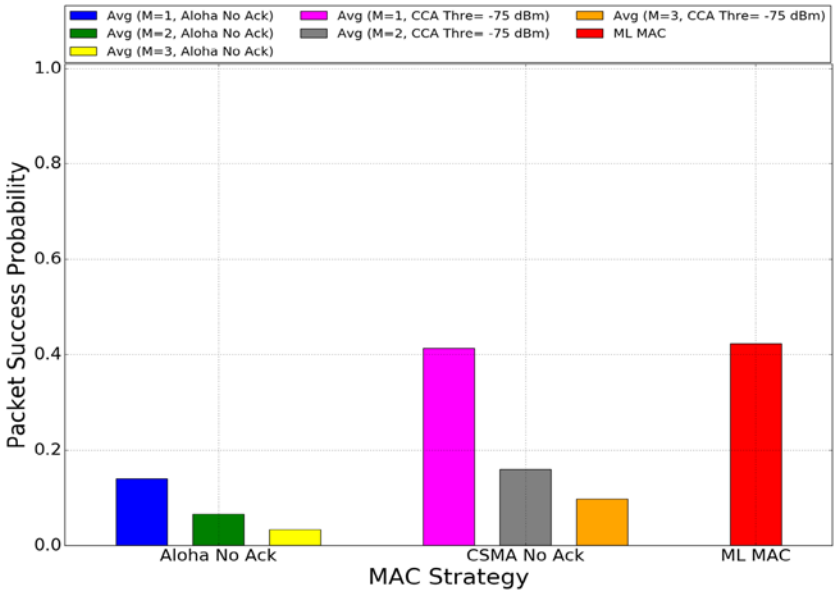


Figure 7.16 : PSP results in a one half dense region

results, with 37% better than Aloha No Ack with K = 3, and 27% better than CSMA No Ack with K = 3. The cognitive MAC also slightly outperforms the CSMA No Ack configuration with K = 1. As shown in Figure 7.18, the PSP fairness follows the same trend as in the same previous high-dense network scenario, and the best PSP fairness results are obtained by the ML MAC configuration.

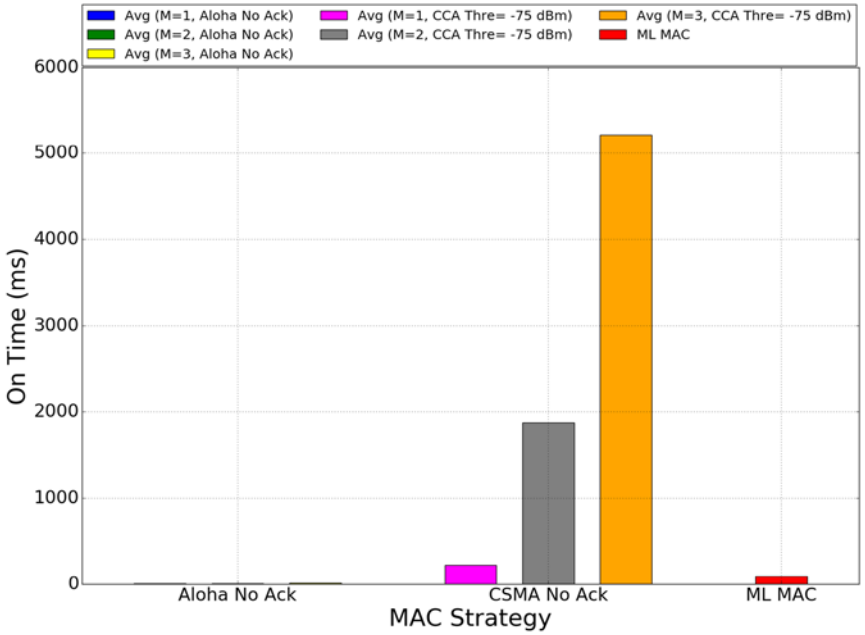


Figure 7.17 : ON time results in a one half dense region

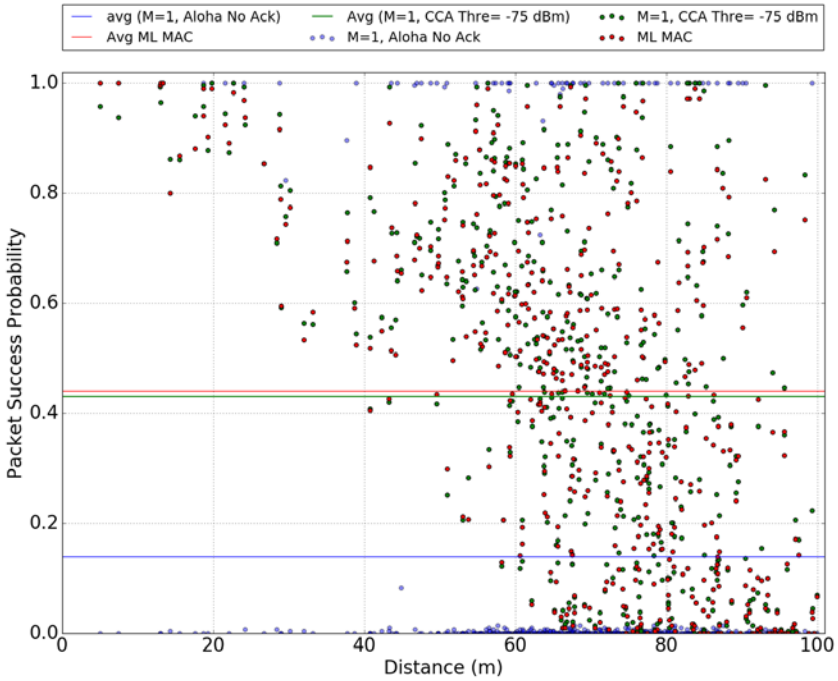


Figure 7.18 : Individual PSP results in a one half dense region

Figure 7.17 shows the average ON time results of all MAC configurations. The two MAC CSMA No Ack configurations with K = 2 and K = 3 are giving, as usual, the longest activity time periods. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC configurations are having perfect ON time fairness results, since all the nodes are getting the same ON time period, as can be observed in Figure 7.19.

The CSMA No Ack with $K = 1$ is the best CSMA based protocol in term of energy efficiency: it gets an ON time average period of nearly 230 ms. In Figure 7.19, we can see the range of values of the latter configuration, that goes from tens of milliseconds to more than 500 ms. The cognitive ML MAC ON time results represent a good compromise between Aloha based MAC configurations and the best CSMA based MAC. The cognitive MAC provides an average ON time period of 90 ms (see Figure 7.19), which is less than half of CSMA No Ack with $K = 1$. The ML MAC solution shows, once again, a binary behavior regarding the ON time fairness. Most of the nodes are having the same ON time duration, close to the average, while a few nodes, unnoticeable on the figure, have a much lower ON time duration (these nodes are configured to use Aloha strategies).

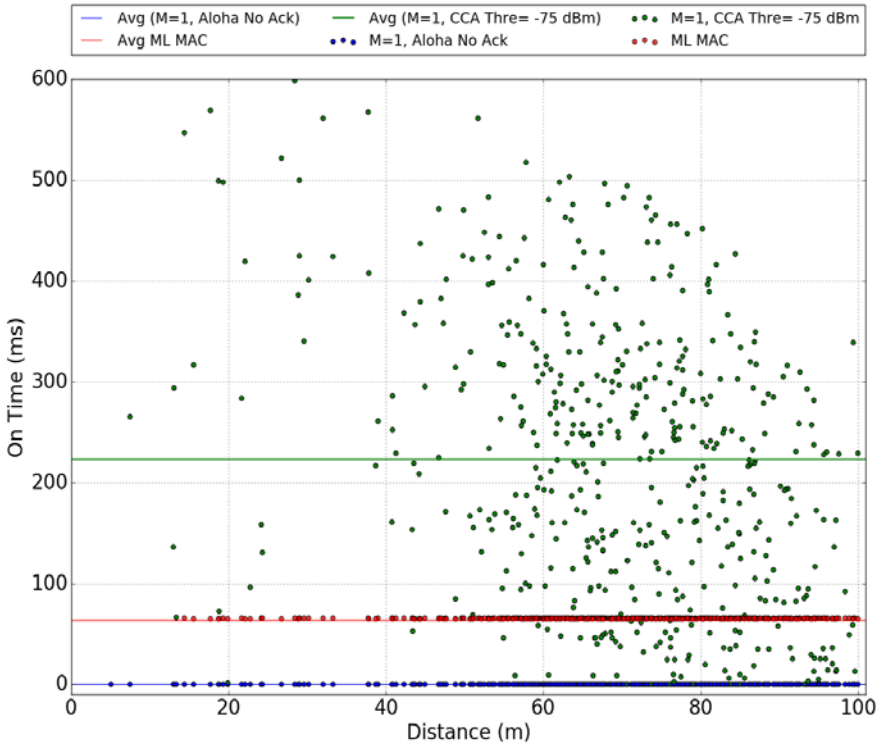


Figure 7.19 : Individual ON time results in a one half dense region

Figure 7.20 shows the MAC configuration distribution of the cognitive ML MAC solution, depicting all the nodes of the cell. We see that the majority of the nodes, 85% of them, are configured at the MAC layer level to use a CSMA No Ack without any frame retransmission ($K = 1$). Some nodes (12% of them) are configured to use Aloha No Ack with $K = 1$. Finally, a few nodes, around 3%, which are the closest to the gateway, are configured to use CSMA No Ack with $K = 3$. The nodes that use Aloha No Ack with $K = 1$ are the furthest nodes from the dense region. Their PSP and ON time performance cannot be enhanced with a carrier sense mechanism due to their position.

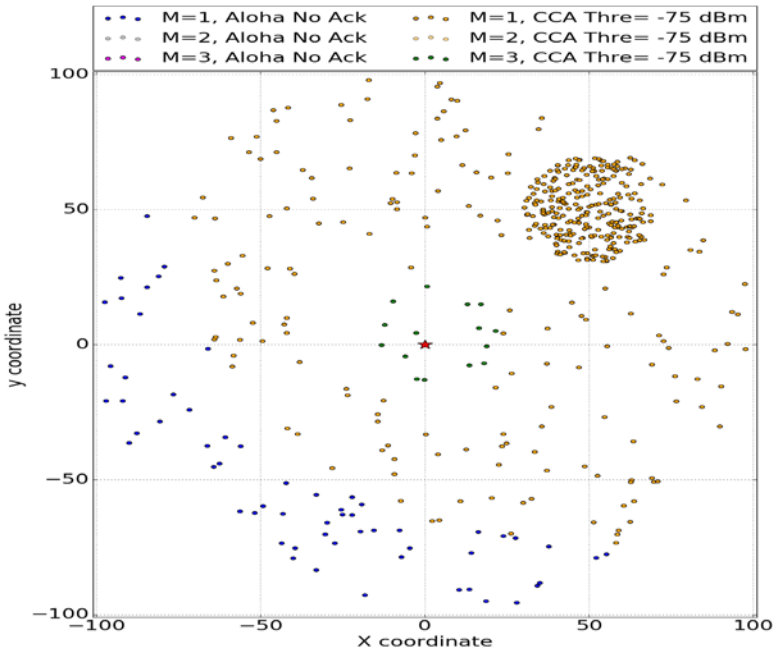


Figure 7.20 : C configuration for ML MAC in a one half dense region

7.2.2.b Medium-dense network

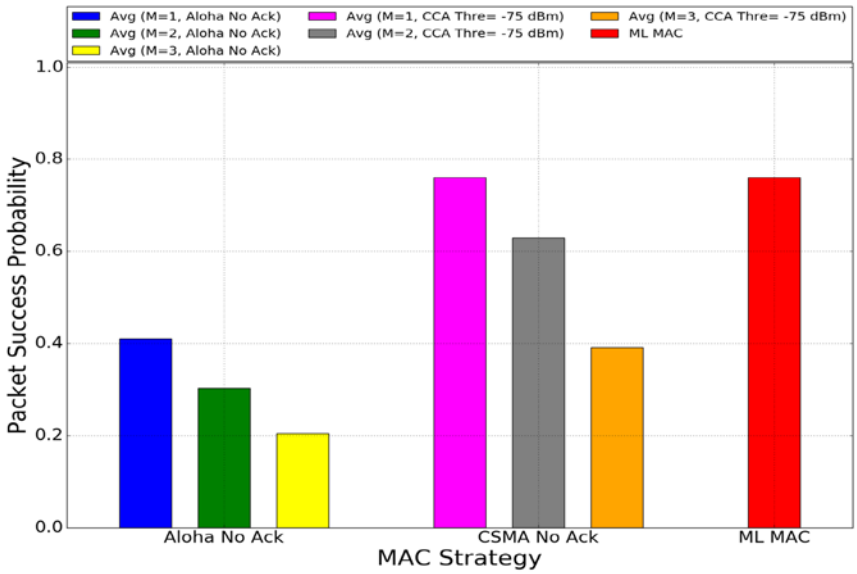


Figure 7.21 : PSP results for a medium-dense network with one dense region

Figure 7.21 shows the average PSP results of all MAC configurations and the PSP obtained by the ML MAC solution. We can see that the CSMA No Ack with $K = 1$ and the ML MAC approach are giving the same, and the highest, PSP result, with 55% better than Aloha No Ack with $K = 3$, and 35% better than CSMA No Ack with $K = 3$.

Figure 7.22 shows the average ON time results of all MAC configurations. It is clear that the longest ON time periods are obtained by CSMA No Ack with $K = 2$ and $K = 3$. Figure 7.23 shows the individual ON Time results for the other MAC configurations. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC

configurations are having a perfect ON time fairness results, since all the nodes are observing the activity time, as we observe in Figure 7.23.

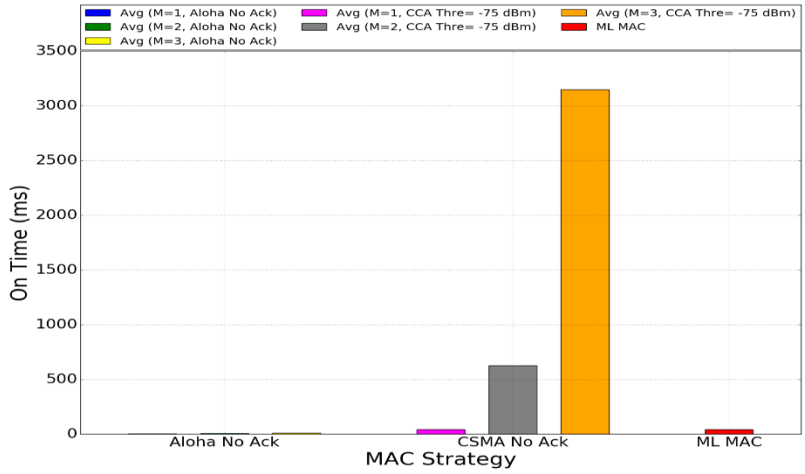


Figure 7.22 : ON time results for a medium-dense network with one dense region

The CSMA No Ack with $K = 1$ is the best CSMA based protocol in terms of energy efficiency, with an ON time average period of nearly 30 ms and a range of values that goes from few milliseconds to 200 ms, as shown in Figure 7.23. For CSMA No Ack with $K = 1$, we have 54% of the nodes getting an ON time shorter than 10 ms, 42% of them with less than 100 ms, and only 4% with an ON time longer than 100 ms.

The cognitive ML MAC strategy for this network density and node distribution is simply to use CSMA No Ack with $K = 1$ for all nodes, since it is the MAC configuration distribution that gives the best compromise between PSP and ON time. The choice of the optimal MAC configuration was simple, just like the previous example of medium-dense network. We, then, do the same as for the one third dense region, and block the CNN algorithm from making this easy choice by forcing it to choose other strategies than CSMA No Ack with $K = 1$. The CNN algorithm will be then proposing a MAC layer configuration that offers the trade-off between all metrics.

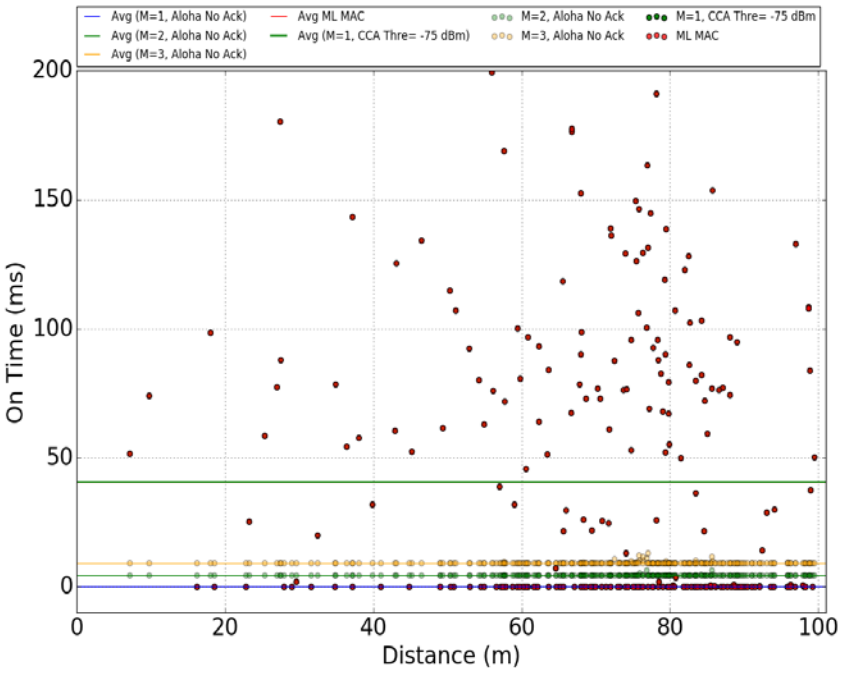


Figure 7.23 : Individual ON time results for a medium-dense network with one dense region

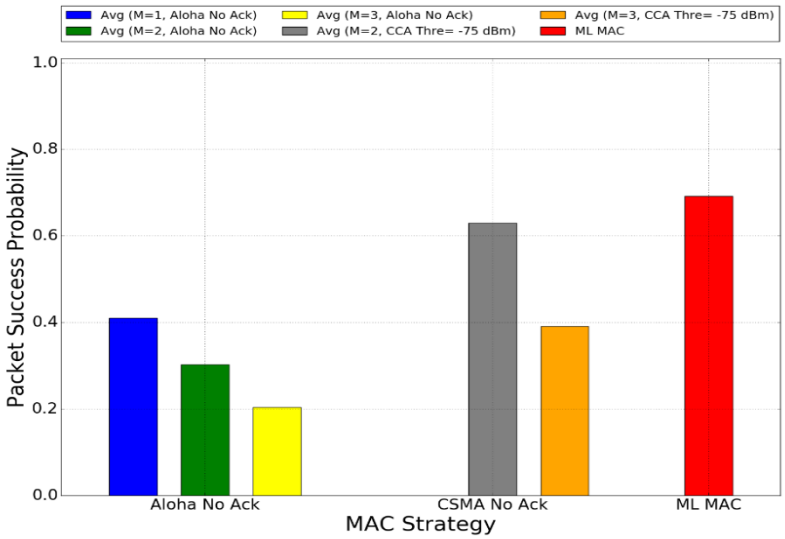


Figure 7.24 : PSP results in a one half dense region without CSMA No Ack with K=1

Figure 7.24 shows the PSP results for ML MAC and those of all the static MAC configurations except for CSMA No Ack with K = 1. The proposed ML MAC has the best average PSP, it outperforms the Aloha No Ack configuration with K = 3 by 47% and CSMA No Ack with K = 3 by 31%. The cognitive MAC is having the best PSP fairness results among all MAC configurations present in this case, as shown in Figure 7.26. This reflects the capacity of our cognitive solution to give the best performance on average while considering a good fairness.

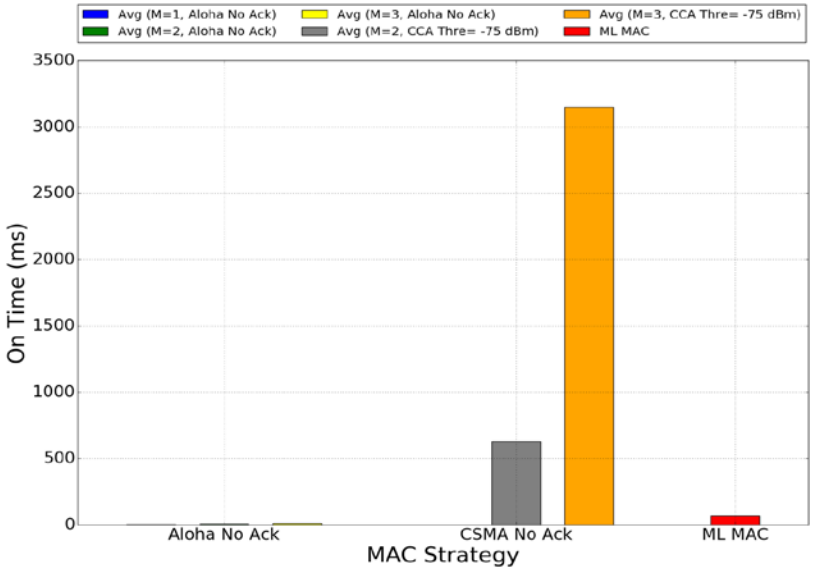


Figure 7.25 : ON time results in a one half dense region without CSMA No Ack with K=1

Figure 7.25 shows the average ON time results of all MAC configurations. It is obvious that the two MAC configurations CSMA No Ack with K = 2 and K = 3 are giving the longest activity time periods. All Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha based MAC configurations are having perfect ON time fairness results, since all the nodes are getting the same activity time. The CSMA No Ack with K = 2 is the best CSMA based protocol in terms of energy efficiency, it gets an ON time average period of nearly 600 ms and a range of values that goes from 100 ms to more than 1000 ms, similarly to the previous medium-dense network scenario. The cognitive MAC ON time results represent a nice compromise between Aloha based

MAC configurations and the best CSMA based MAC. The cognitive ML MAC provides an average ON time period of 65 ms, which is almost ten times less than CSMA No Ack with $K = 2$.

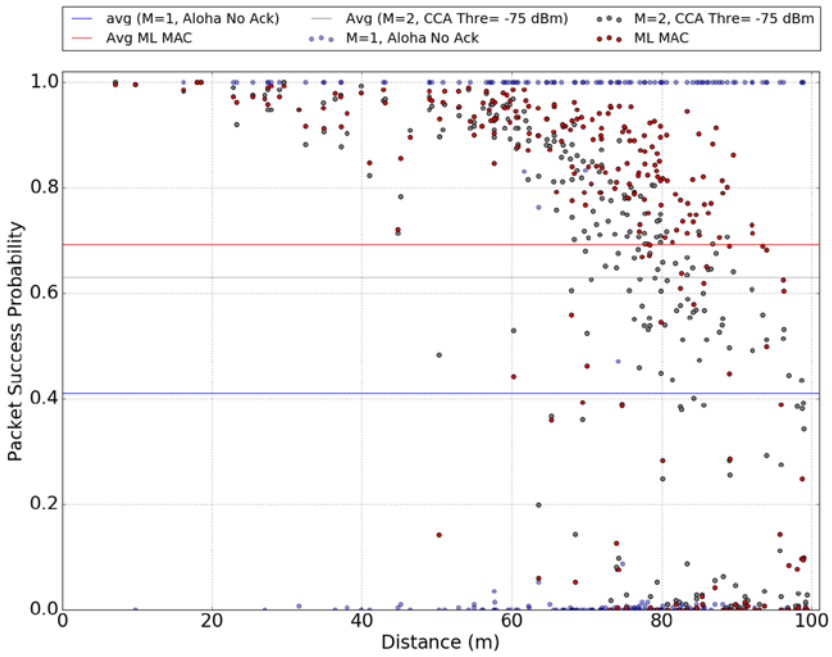


Figure 7.26 : Individual PSP results in a one half dense region without CSMA No Ack with K=1

Figure 7.27 shows the MAC configuration distribution for the cognitive ML MAC solution. We see that the majority of the nodes, 82% of them, are configured at the MAC layer to use CSMA No Ack with $K = 2$, 16% of the nodes are configured to use Aloha No Ack with $K = 1$, while only 2% of the nodes are configured with CSMA No Ack with $K = 3$. The nodes that use Aloha No Ack with $K = 1$ are those furthest away with respect to the dense region, whose PSP and ON time performance could not be enhanced even by activating the carrier sense mechanism, due to their position. The nodes that use CSMA No Ack with $K = 3$ at the MAC layer are the closest to the gateway. The choice

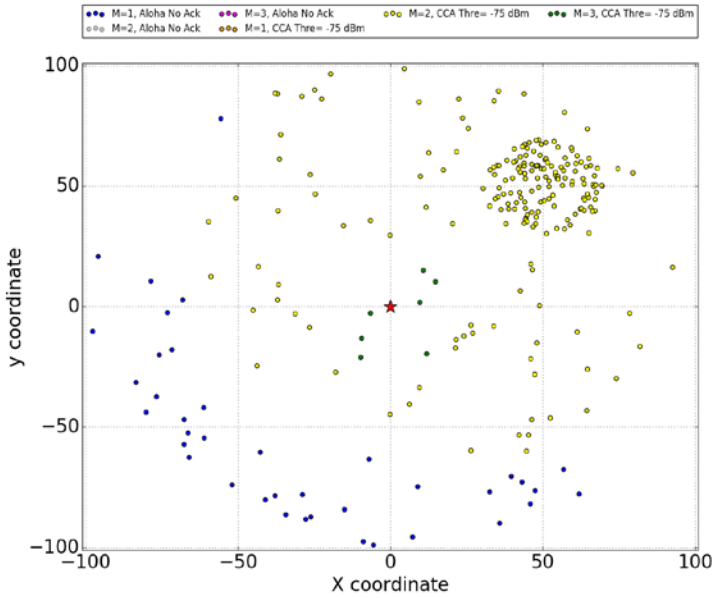
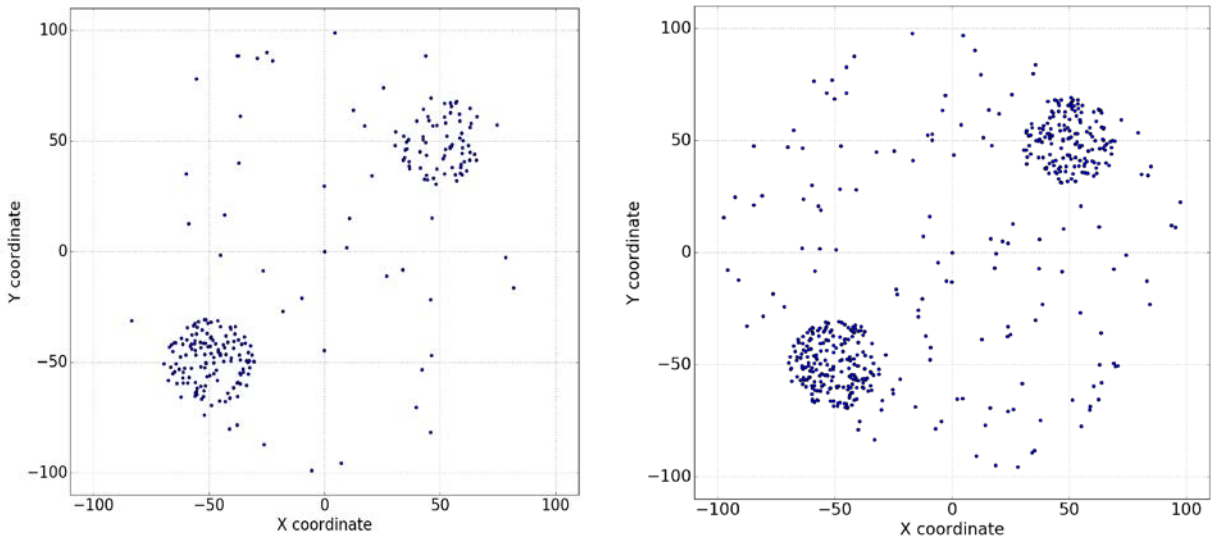


Figure 7.27 : MAC configuration for ML MAC in a one half dense region

of retransmitting three times is because of the high CCA conflict rate of these nodes: to increase their chances to access the channel, the ML MAC makes them retransmit more than other nodes.

7.2.3 Two dense regions

We apply here another non uniform distribution, where we have two dense regions in a cell: one region that contains the third of the cell nodes, the other region that contains the half of the cell nodes, and the remainder of the cell contains the rest of the nodes scattered. Figure 7.28 shows the node distribution used in this section for both medium-dense and high dense networks. We simulated networks of 250 and 500 nodes, which respectively represent a medium-dense and a high-dense network.



(a) 250 Nodes

(b) 500 Nodes

Figure 7.28 : Two third dense region for networks of 250 and 500 nodes

7.2.3.a High-dense network

Figure 7.29 shows the average PSP results of all MAC configurations, as well as the PSP obtained by the ML MAC solution. We can see that the CSMA No Ack with $K = 1$ and the ML MAC are giving the same, and the highest, PSP results on average, with 32% better than Aloha No Ack with $K = 3$, and 28% better than CSMA No Ack with $K = 3$.

Figure 7.30 shows the average ON time results for all MAC configurations. The two CSMA No Ack configurations with $K = 2$ and $K = 3$ have the longest activity time periods on average. In Figure 7.31 we zoom on the ON time results for the best energy saving MAC configurations. We can see that all Aloha based MAC configurations have very short ON time periods, less than 10 ms. Aloha based MAC configuration also have perfect ON time fairness results, since all the nodes are giving the same ON time period. The CSMA No Ack with $K = 1$ is the best CSMA based protocol in terms of energy efficiency, with an ON time average period of nearly 150 ms and a range of value that goes from a few milliseconds to 200 ms. The cognitive ML MAC outperforms CSMA No Ack with $K = 1$ in terms of ON time periods, since it has an activity time of less than 100 ms on average.

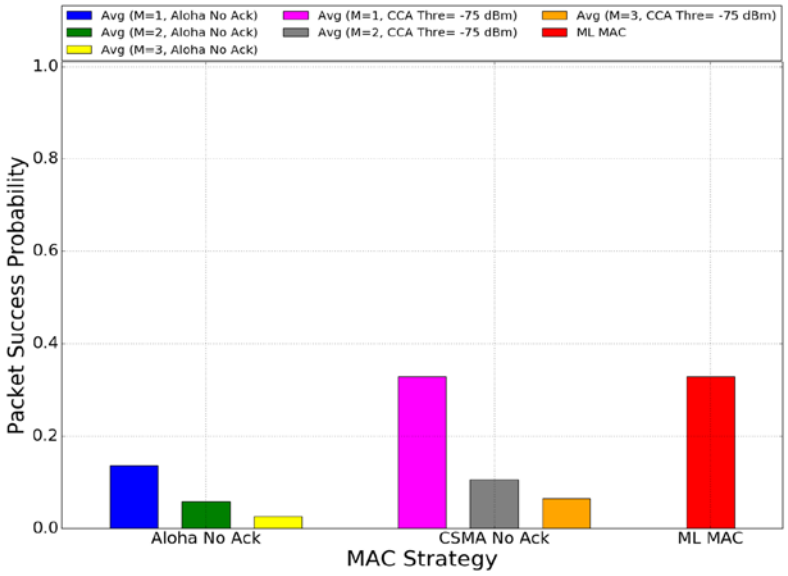


Figure 7.29 : PSP results for a deployment with two dense regions

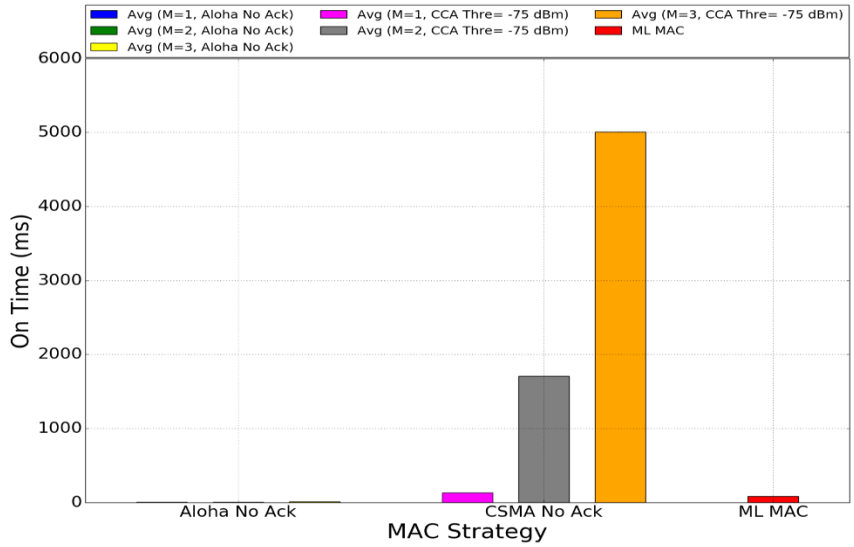


Figure 7.30 : ON time results for a deployment with two dense regions

Figure 7.32 shows the MAC configuration distribution of the cognitive ML MAC solution, depicting the choice of the CCN algorithm for each node of the cell. We see that the majority of the nodes, 98% of them, are configured at the MAC layer level to use CSMA No Ack without any frame retransmission (K = 1). The rest of the nodes, 2% of the toal, are configured with CSMA No Ack and K = 3. Those are nodes very close to the gateway, and this configuration is chosen for them for the same aforementioned reasons.

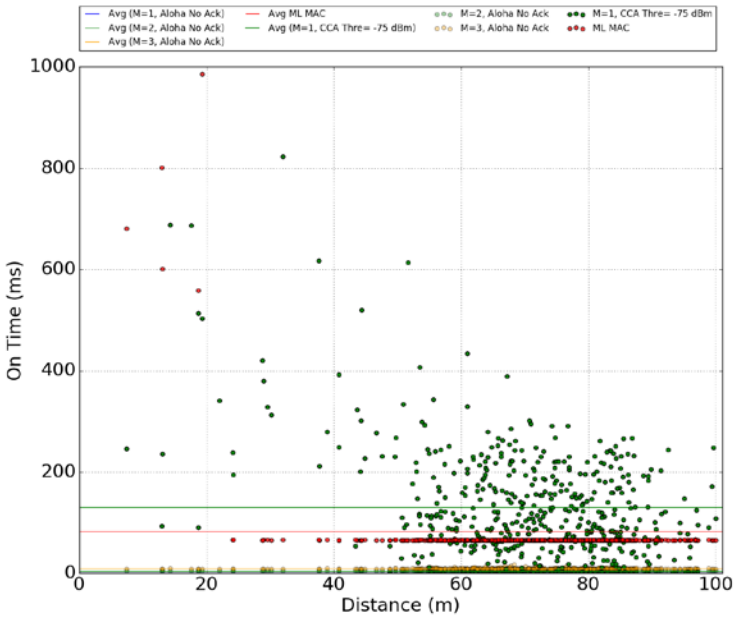


Figure 7.31 : Individual ON time results for a deployment with two dense regions

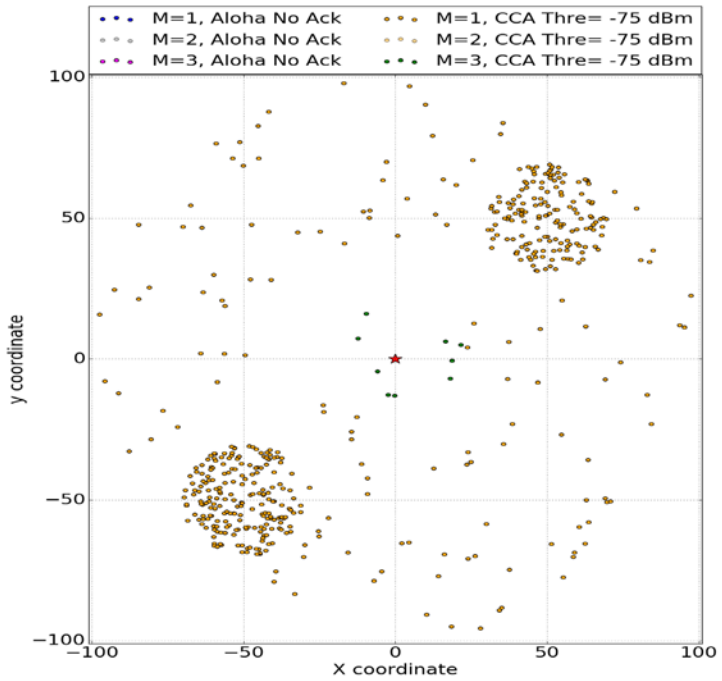


Figure 7.32 : MAC configuration for ML MAC with two dense regions

7.2.3.b Medium-dense network

Figure 7.33 shows the average PSP results of all MAC configurations and the PSP obtained by the ML MAC solution. We can see that the ML MAC is giving the highest PSP result, with 54% better than Aloha No Ack with $K = 3$, and 47% better than CSMA No Ack with $K = 3$. The ML solution outperforms the CSMA No Ack configuration with $K = 1$ by 6% on average, while also giving a slightly better PSP fairness among the nodes.

Figure 7.34 shows the ON time results of all MAC configurations. Once again, the two MAC configurations using CSMA No Ack with $K = 2$ and $K = 3$ are giving the longest activity time periods.

In Figure 7.35 we show the ON time results for the remaining protocols. We can see that all Aloha based MAC configurations are having very short ON time periods, less than 10 ms. Aloha

based MAC configuration are having perfect ON time fairness results, since all the nodes are getting the same ON time period.

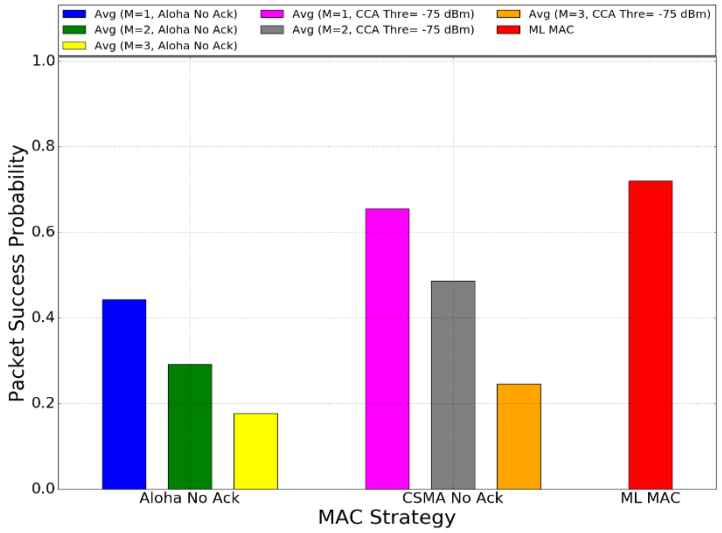


Figure 7.33 : PSP results for a medium-dense deployment with two dense regions

The cognitive ML MAC gives slightly better results energy-wise, with an average activity time of 30 ms.

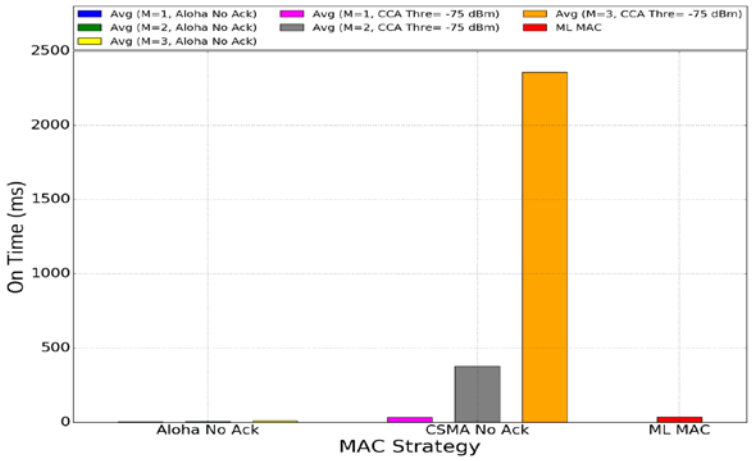


Figure 7.34 : ON time results for a medium-dense deployment with two dense regions

Figure 7.36 shows the MAC configuration distribution for the cognitive ML MAC solution for every node of the cell. We see that the majority of the nodes, 90% of them, are configured at the MAC layer level to use CSMA No Ack without any frame retransmission (K = 1). The rest of the nodes, 10% of the toal, are configured with CSMA No Ack and K = 2. Those are nodes very close to the gateway, and this configuration is chosen for them for the same aforementioned reasons. Some nodes configured with CSMA No Ack and K = 2 are located inside the dense region that contains half of the nodes of the cell, and that could be due to a very low PSP obtained with K = 1 because of their lower chance to access to the channel, so the machine-learning technique tackles this by multiplying the number of frames to send at the MAC layer.

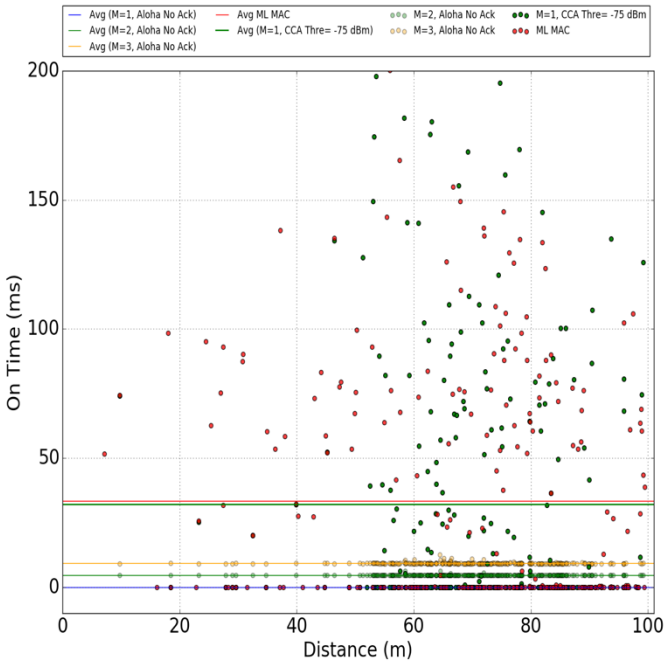


Figure 7.35 : Individual ON time results for a medium-dense deployment with two dense regions

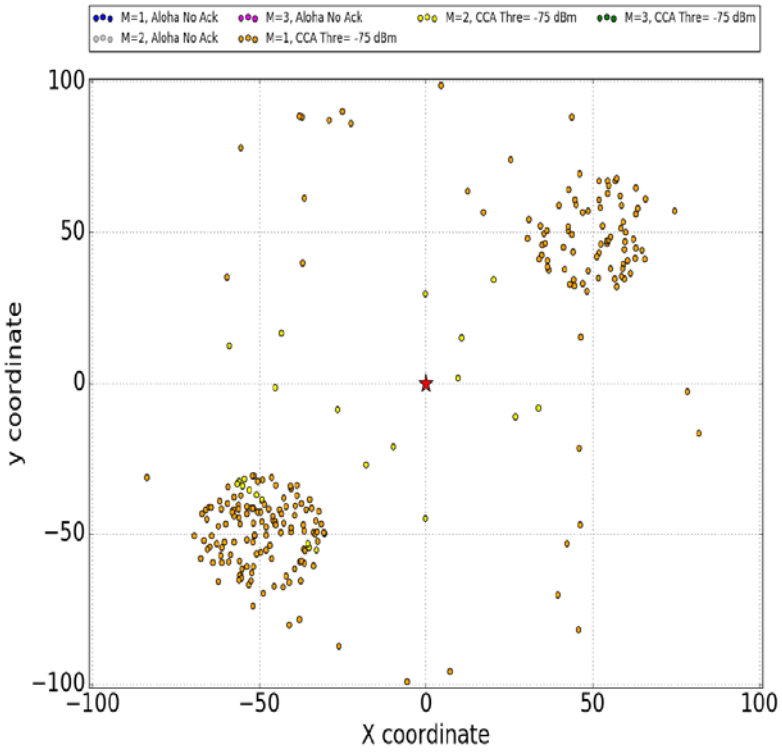


Figure 7.36 : MAC configuration for ML MAC with two dense regions

7.3 Conclusion

In this chapter, we modified our machine learning algorithm to accomodate more realistic conditions. We first removed the distance separating the node to the gateway from the input data set, considering this information is a hard to obtain in a real LPWAN network. We replaced this

information by the ON time observed by the node. Then, we used non uniform node distributions to analyze a higher realism in terms of deployment. We showed how the CNN algorithm proposed smart combinations of MAC configurations, improving network performance in terms of packet success probability and energy saving, while adapting to all kinds of network topologies.

8. Conclusions and future perspectives

In this chapter, we conclude this manuscript with a summary of our contributions and we discuss the open perspectives for future work.

8.1 Conclusions

Throughout this thesis, we propose a cognitive MAC solution for dedicated IoT networks, which builds on Convolutional Neural Network techniques to improve the network performance in terms of packet success probability and energy consumption.

In Chapter 2, we survey the field of IoT networks and we present the solutions offered by different IoT players. We also discuss the role of the MAC layer and present the most relevant enhancements proposed in the literature. We address the different MAC solutions used by multiple IoT technology providers. At the end of this chapter, we briefly introduce machine learning techniques and survey their applications in the networking field in general, in the MAC layer and in MAC layer for IoT networks in particular.

Chapter 3 discusses MAC layer solutions for dedicated IoT networks and evaluates them through ns3 simulations. We show that the best MAC layer approach depends on parameters such as the number of competing nodes and the packet arrival rate. In addition, we remark that using acknowledgement messages can have a negative impact, always reducing the network performance in terms of reliability and energy consumption. This supports our belief that the MAC strategy for dedicated IoT networks needs to adapt to the network state and to the target metric. Moreover, depending on the local traffic density, different MAC solutions can be used in different parts of the cell, orchestrated by a smart gateway.

In Chapter 4, we study the performance of the Aloha MAC protocol through simulations and analytical modeling. We limited the study to the specific case of an Aloha protocol without the use of acknowledgment messages, denoted Aloha No Ack, which is used by most LPWAN technologies. In the chapter, we focus on the frame retransmission number, one of the MAC layer parameters. We study this using an original analytical model, which allows us to show how the network performance changes with the variation of this parameter under different network conditions. Afterward, we exploit the analytical model to get the optimal value for frame retransmissions in each network condition. Interestingly, the optimal value in many cases does not correspond to the highest number of retransmissions, which means redundancy does not always imply better reliability. At the end of the chapter, we compare the performances obtained by Aloha No Ack with an optimal number of frame retransmissions and the Aloha flavor used by SigFox. The results showed, under many traffic conditions, the significant underperformance of the static MAC configuration used by SigFox, in terms of both reliability and energy consumption.

In Chapter 5, we studied the performance of the CSMA No Ack based MAC protocol for LPWAN. Our study focused on the CCA threshold parameter, which reflects the sensitivity of the receiver. We showed with extensive simulation results how this parameter impacts the network performance in terms of packet success probability and node activity time. Then, we introduced the CCA conflict rate metric, which represents the percentage of contenders that a node is enable to hear, and it allows us to deduce the percentage of hidden stations for each node. Afterward, we showed how a correlation exists, in many cases, between the CCA conflict rate and the performance metrics (packet success probability and node activity time). Moreover, for the CSMA No Ack case, we conducted a study on the impact of the frame retransmission number on the network performance. We concluded that, for all CCA threshold values, when no frame retransmission is used, the network performed. Then, by using realistic settings for the CCA threshold parameter, we produced a comparison between Aloha

No Ack and CSMA No Ack, both using their optimal number of retransmissions. We showed how CSMA No Ack has better reception probability all the time, but with longer node activity period, and we showed how sometimes a good compromise could be achieved by CSMA No Ack with a reduced number of retransmissions.

To the best of our knowledge, this is the first contribution that consider the impact of the CCA threshold while studying the implementation of the CSMA protocol for LPWANs. Also, this is the first work that introduces the CCA conflict rate metric and proposes a realistic evaluation of CSMA, demonstrating a good compromise between reliability and energy consumption compared to Aloha based networks.

In Chapter 6, we present our machine learning based MAC solution for dedicated IoT networks. We showed how our proposed solution is capable of taking advantage of both classic MAC approaches, Aloha and CSMA, by allowing their coexistence within the same cell. Our solution takes into consideration the transmission reliability, energy consumption and fairness between the cell nodes. This contribution is the fruit of the evaluation conducted in previous chapters, which allowed us to identify key parameters that need to be tuned dynamically in order to give the best network performance. Through simulation results, we showed the enhancements in terms of packet success probability and activity time period that could be obtained with a machine learning based MAC. For a loaded network, the success probability gain obtained by the ML MAC with respect to static MAC configurations reflects a promise of a better scalability for dedicated IoT networks. To the best of our knowledge, this is the first work that proposes a cognitive MAC solution for dedicated IoT networks.

In Chapter 7, we evaluate our machine learning algorithm in more realistic conditions. We first removed the distance separating the node to the gateway from the input data set, considering this is an information hard to obtain in a real LPWAN network. We replaced this information by the activity time observed by the node. Then, we used non uniform spatial node distributions to reach a higher realism in terms of deployment. We showed how the CNN algorithm reached smart combinations of MAC configurations, improving network performance in terms of packet success probability and energy savings, while adapting to all kinds of network topologies.

8.2 Future perspectives

The work presented in this thesis focuses on proposing a cognitive MAC protocol, which can be seen as a tunable MAC protocol, where the different MAC parameters progress as the network conditions change. This work can be improved with the inclusion of other MAC layer parameters. For example, the CSMA approach can be improved with the dynamic adaptation of the contention window size and of the backoff exponent, which was tested in previous contributions, but for a different context [87][89]. We believe this latter conclusion is worth to test in our context and that it could enrich our contribution.

The IoT network ensures the connections of all types of objects to the Internet. These objects can be static and also mobile, hence adding mobility schemes to the simulations would make their results closer to a real-life IoT network, which would strengthen our conclusions. The mobility of IoT networks is another fertile field for machine learning techniques, allowing for the mobility prediction of the devices and thus the prediction of the network state. The mobility prediction is a complex problem, since objects of different nature will be connected to the network. We can exploit mobile networks data in order to train a machine learning solution regarding IoT device mobility, since mobile data mobility is a combination of different ways of transport used by the mobile user. Moreover, a mobility prediction solution can precede the cognitive MAC solution, in order to provide it with the predicted device distribution as input.

One of the first conclusions of this thesis states that the usage of acknowledgement messages does not bring benefits to the IoT network performance. Anyway, the acknowledgement messages are still present in a limited way in IoT technology provider solutions. Hence, adding the capacity of coexistence of MAC configurations using partial acknowledgements could enrich the simulation work. Especially, if for some applications the devices need a downlink feedback from the gateway, even though limited.

The results shown in this thesis present a promise of efficiency of machine learning techniques for a MAC layer suitable for dedicated IoT networks. However, these results are mainly simulation results. The thesis contribution needs real experimental work proving the accuracy of the conclusions obtained based on the simulation and analytical results. A collaboration can be done with colleagues working on the implementation of a LoRa network on the campus, in order to dedicate a sub-network as a pilot machine learning based network. Otherwise, the implementation of our cognitive MAC solution for short-range networks could also be seen as a small scale experimental proof of concept. However, such a study must be well conducted in order to adapt the transmission power of the sensors and the dimension of the sensor-based model in order to be representative to a real LPWAN.

Finally, in this thesis, we considered the case of one IoT cell, and supposed to exploit the history of this cell in order to build the machine learning model. We also supposed that the machine learning logic would be executed at the gateway station. However, enhancements can be done at this level if we send data generated from multiple gateways to a dedicated server that performs predictions based on historical data coming from multiple IoT cells. To do so, some changes and adaptations of our machine learning solution would be required.

References

[1] Quinlan, J. Ross. C4. 5: programs for machine learning. Elsevier, 2014.
[2] SINCLAIR, Chris, PIERCE, Lyn, et MATZNER, Sara. An application of machine learning to network intrusion detection. In : Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99). IEEE, 1999. p. 371-377.
[3] SHON, Taeshik et MOON, Jongsub. A hybrid machine learning approach to network anomaly detection. Information Sciences, 2007, vol. 177, no 18, p. 3799-3821.
[4] MÄHÖNEN, Petri, PETROVA, Marina, RIIHIJÄRVI, Janne, et al. Cognitive wireless networks: Your network just became a teenager. In : Proceedings of the INFOCOM. 2006. p. 23-29.
[5] CLANCY, Charles, HECKER, Joe, STUNTEBECK, Erich, et al. Applications of machine learning to cognitive radio networks. IEEE Wireless Communications, 2007, vol. 14, no 4, p. 47-52.
[6] ALSHEIKH, Mohammad Abu, LIN, Shaowei, NIYATO, Dusit, et al. Machine learning in wireless sensor networks: Algorithms, strategies, and applications. IEEE Communications Surveys & Tutorials, 2014, vol. 16, no 4, p. 1996-2018.
[7] JIANG, Chunxiao, ZHANG, Haijun, REN, Yong, et al. Machine learning paradigms for next-generation wireless networks. IEEE Wireless Communications, 2016, vol. 24, no 2, p. 98-105.
[8] KIBRIA, Mirza Golam, NGUYEN, Kien, VILLARDI, Gabriel Porto, et al. Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. IEEE access, 2018, vol. 6, p. 32328-32338.
[9] DOERR, Christian, NEUFELD, Michael, FIFIELD, Jeff, et al. MultiMAC-an adaptive MAC framework for dynamic radio networking. In : First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. IEEE, 2005. p. 548-555.
[10] SHA, Mo, DOR, Rahav, HACKMANN, Gregory, et al. Self-adapting mac layer for wireless sensor networks. In : 2013 IEEE 34th Real-Time Systems Symposium. IEEE, 2013. p. 192-201.
[11] RAJAB, Samer A., BALID, Walid, AL KALAA, Mohamad O., et al. Energy detection and machine learning for the identification of wireless MAC technologies. In : 2015 international wireless communications and mobile computing conference (IWCMC). IEEE, 2015. p. 1440-1446.
[12] AL-KASEEM, Bilal R., AL-RAWESHIDY, Hamed S., AL-DUNAINAWI, Yousif, et al. A new intelligent approach for optimizing 6LoWPAN MAC layer parameters. IEEE Access, 2017, vol. 5, p. 16229-16240.
[13] U. Raza, P. Kulkarni, M. Sooriyabandara, “Low Power Wide Area Networks: An Overview”, IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855–873, Apr. 2017.
[14] Y. Mo, C. Goursaud, J.M. Gorce, “Theoretical Analysis of UNB-based IoT Networks with Path Loss and Random Spectrum Access”, Proc. IEEE PIMRC 2016, Valencia, Spain, Sep. 2016.
[15] O. Iova, A.L. Murphy, G.P. Picco, L. Ghiro, D. Molteni, F. Ossi, F. Cagnacci, “LoRa from the City to the Mountains: Exploration of Hardware and Environmental Factors”, Proc. MadCom 2017, Uppsala, Sweden, Feb. 2017.
[16] E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, H.S. Razaghi, “A Primer on 3GPP Narrowband Internet of Things”, IEEE Communications Magazine, vol. 55, no. 3, pp. 117–123, Mar. 2017.
[17] T. Adame, A. Bel, B. Bellalta, J. Barcelo, M. Oliver, “IEEE 802.11ah: The WiFi Approach for M2M Communications”, IEEE Wireless Communications, vol. 21, no. 6, pp. 144–152, Dec. 2014.
[18] M. Lauridsen, I.Z. Kovacs, P. Mogensen, M. Sorensen, S. Holst, “Coverage and Capacity Analysis of LTE-M and NB-IoT in a Rural Area”, Proc. IEEE VTC Fall, Montreal, QC, Canada, Sep. 2016.
[19] S. Cherkaoui, I. Keskes, H. Rivano, R. Stanica, “LTE-A Random Access Channel Capacity Evaluation for M2M Communications”, Proc. IFIP WD, Toulouse, France, Mar. 2016.
[20] L Kleinrock, F.A. Tobagi, “Packet switching in radio channels: Part I–Carrier sense multiple-access modes and their throughput-delay characteristics”, IEEE transactions on Communications, vol. 23, no 12, p. 1400-1416, Dec. 1975.

[21] B. Blaszczyszyn, P. Muhlethaler, S. Banaouas, “A Comparison of ALOHA and CSMA in Wireless Ad Hoc Networks under Different Channel Conditions”, Inria Research Report 00530093, Oct. 2010.
[22] A. Boubrima, F. Matigot, W. Bechkit, H. Rivano, A. Ruas, “Optimal Deployment of Wireless Sensor Networks for Air Pollution Monitoring”, Proc. ICCCN, Las Vegas, NV, USA, Aug. 2015.
[23] R. Domga Komguem, R. Stanica, M. Tchuente, F. Valois, “WARIM: Wireless Sensor Network Architecture for a Reliable Intersection Monitoring”, Proc. IEEE ITSC, Qingdao, PRC, Oct. 2014.
[24] T. Saadawi, A. Ephremides, “Analysis, Stability and Optimisation of Slotted Aloha with a Finite Number of Buffered Users”, IEEE Transactions on Automatic Control, vol. 26, no. 3, pp. 680–689, Jun. 1981.
[25] D. Raychaudhuri, K. Joseph, “Performance Evaluation of Slotted Aloha with Generalized Retransmission Backoff”, IEEE Transactions on Communications, vol. 38, no. 1, pp. 117–122, Jan. 1990.
[26] L. Dai, “Toward a Coherent Theory of CSMA and Aloha”, IEEE Transactions on Wireless Communications, vol. 12, no. 7, pp. 3428–3444, Jul. 2013.
[27] Y. Yang, T.-S. Yum, “Delay Distributions of Slotted ALOHA and CSMA”, IEEE Transactions on Communications, vol. 51, no. 11, pp. 1846–1857, Nov. 2003.
[28] F. Baccelli, B. Blaszczyszyn, P. Muhlethaler, “Stochastic Analysis of Spatial and Opportunistic Aloha”, IEEE Journal of Selected Areas in Communications, vol. 27, no. 7, pp. 1105–1119, Sep. 2009.
[29] A. Sakata, T. Yamazato, H. Okada, M. Katayama, “Throughput Comparison of CSMA and CDMA slotted ALOHA in Inter-Vehicle Communication”, Proc. ITST, Sophia Antipolis, France, Jun. 2007.
[30] Z. Li, S. Zozor, J.-M. Drossier, N. Varsier, Q. Lampin, “2D Time-Frequency Interference Modelling using Stochastic Geometry for Performance Evaluation in Low-Power Wide-Area Networks”, Proc. IEEE ICC, Paris, France, May 2017.
[31] Q. Song, X. Lagrange, L. Nuyami, “An Analytical Model for S-ALOHA Performance Evaluation in M2M Networks”, Proc. IEEE ICC, Paris, France, May 2017.
[32] X. Ma, X. Chen, “Performance Analysis of IEEE 802.11 Broadcast Scheme in Ad Hoc Wireless LANs”, IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3757–3768, Nov. 2008.
[33] ABRAMSON, Norman. THE ALOHA SYSTEM: another alternative for computer communications. In : Proceedings of the November 17-19, 1970, fall joint computer conference. 1970. p. 281-285.
[34] CROWTHER, Will, RETTBERG, R., WALDEN, D., et al. A system for broadcast communication: Reservation-ALOHA. In : Proc. 6th Hawaii Int. Conf. Syst. Sci. 1973. p. 596-603.
[35] MAKRAKIS, Dimitrios et MURTHY, K.. M.. Sundara . Spread slotted ALOHA techniques for mobile and personal satellite communication systems. IEEE Journal on Selected Areas in Communications, 1992, vol. 10, no 6, p. 985-1002.
[36] BACCELLI, Francois, BLASZCZYSZYN, Bartlomiej, et MÜHLETHALER, Paul. A spatial reuse Aloha MAC protocol for multihop wireless mobile networks. 2003.
[37] BACCELLI, François, BLASZCZYSZYN, Bartlomiej, et MUHLETHALER, Paul. An Aloha protocol for multihop mobile wireless networks. IEEE Transactions on Information Theory, 2006, vol. 52, no 2, p. 421-436.
[38] GOODMAN, DAVID J. et SALEH, Adel AM. The near/far effect in local ALOHA radio communications. IEEE Transactions on vehicular technology, 1987, vol. 36, no 1, p. 19-27.
[39] RAYCHAUDHURI, Dipankar et JOSEPH, Kuriacose. Performance evaluation of slotted ALOHA with generalized retransmission backoff. IEEE Transactions on Communications, 1990, vol. 38, no 1, p. 117-122.
[40] FERRÉ, Guillaume et SIMON, Eric. An introduction to Sigfox and LoRa PHY and MAC layers. 2018.

[41] GOURSAUD, Claire et MO, Yuqi. Random unslotted time-frequency ALOHA: Theory and application to IoT UNB networks. In : 2016 23rd International Conference on Telecommunications (ICT). IEEE, 2016. p. 1-5.
[42] GHEZ, Sylvie, VERDU, Sergio, et SCHWARTZ, Stuart C. Stability properties of slotted Aloha with multipacket reception capability. IEEE transactions on automatic control, 1988, vol. 33, no 7, p. 640-649.
[43] KOSUNALP, Selahattin, MITCHELL, Paul D., GRACE, David, et al. Experimental study of capture effect for medium access control with ALOHA. ETRI Journal, 2015, vol. 37, no 2, p. 359-368.
[44] BANKOV, Dmitry, KHOROV, Evgeny, et LYAKHOV, Andrey. Mathematical model of LoRaWAN channel access with capture effect. In : 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017. p. 1-5.
[45] MIKHAYLOV, Konstantin, PETAEJAEJAERVI, Juha, et HAENNINEN, Tuomo. Analysis of capacity and scalability of the LoRa low power wide area network technology. In : European Wireless 2016; 22th European Wireless Conference. VDE, 2016. p. 1-6.
[46] MAGRIN, Davide, CENTENARO, Marco, et VANGELISTA, Lorenzo. Performance evaluation of LoRa networks in a smart city scenario. In : 2017 IEEE International Conference on communications (ICC). ieee, 2017. p. 1-7.
[47] GEORGIOU, Orestis et RAZA, Usman. Low power wide area network analysis: Can LoRa scale?. IEEE Wireless Communications Letters, 2017, vol. 6, no 2, p. 162-165.
[48] SLABICKI, Mariusz, PREMSANKAR, Gopika, et DI FRANCESCO, Mario. Adaptive configuration of LoRa networks for dense IoT deployments. In : NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018. p. 1-9.
[49] HATA, Masaharu. Empirical formula for propagation loss in land mobile radio services. IEEE transactions on Vehicular Technology, 1980, vol. 29, no 3, p. 317-325.
[50] KIM, Seong-Cheol, GUARINO, B. J., WILLIS, T. M., et al. Radio propagation measurements and prediction using three-dimensional ray tracing in urban environments at 908 MHz and 1.9 GHz. IEEE Transactions on Vehicular Technology, 1999, vol. 48, no 3, p. 931-946.
[51] DURGIN, Greg, PATWARI, Neal, et RAPPAPORT, Theodore S. An advanced 3D ray launching method for wireless propagation prediction. In : 1997 IEEE 47th Vehicular Technology Conference. Technology in Motion. IEEE, 1997. p. 785-789.
[52] HOSSEINZADEH, Salaheddin, ALMOATHEN, Mahmood, LARIJANI, Hadi, et al. A neural network propagation model for LoRaWAN and critical analysis with real-world measurements. Big Data and Cognitive Computing, 2017, vol. 1, no 1, p. 7.
[53] EL CHALL, Rida, LAHOUD, Samer, et EL HELOU, Melhem. LoRaWAN network: radio propagation models and performance evaluation in various environments in Lebanon. IEEE Internet of Things Journal, 2019, vol. 6, no 2, p. 2366-2378.
[54] LI, Zhuocheng, ZOZOR, Steeve, BROSSIER, Jean-Marc, et al. 2D Time-frequency interference modelling using stochastic geometry for performance evaluation in Low-Power Wide-Area Networks. In : 2017 IEEE International Conference on Communications (ICC). IEEE, 2017. p. 1-7.
[55] SASTRY, A. Effect of acknowledgment traffic on the performance of slotted ALOHA-code division multiple access systems. IEEE transactions on communications, 1984, vol. 32, no 11, p. 1219-1222.
[56] KYASANUR, Pradeep et VAIDYA, Nitin H. Capacity of multi-channel wireless networks: impact of number of channels and interfaces. In : Proceedings of the 11th annual international conference on Mobile computing and networking. 2005. p. 43-57.
[57] CROW, Brian P., WIDJAJA, Indra, KIM, Jeong Geun, et al. IEEE 802.11 wireless local area networks. IEEE Communications magazine, 1997, vol. 35, no 9, p. 116-126.
[58] BIANCHI, Giuseppe. Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal on selected areas in communications, 2000, vol. 18, no 3, p. 535-547.

[59] LACAGE, Mathieu, MANSHAEI, Mohammad Hossein, et TURLETTI, Thierry. IEEE 802.11 rate adaptation: a practical approach. In : Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems. 2004. p. 126-134.
[60] PHAM, Congduc. Robust CSMA for long-range LoRa transmissions with image sensing devices. In : 2018 Wireless Days (WD). IEEE, 2018. p. 116-122.
[61] KOUVELAS, Nikos, RAO, Vijay, et PRASAD, R. R. Employing p-csma on a lora network simulator. arXiv preprint arXiv:1805.12263, 2018.
[62] ZUCCHETTO, Daniel et ZANELLA, Andrea. Uncoordinated access schemes for the IoT: approaches, regulations, and performance. IEEE Communications Magazine, 2017, vol. 55, no 9, p. 48-54.
[63] TO, Thanh-Hai et DUDA, Andrzej. Simulation of lora in ns-3: Improving lora performance with csma. In : 2018 IEEE International Conference on Communications (ICC). IEEE, 2018. p. 1-7.
[64] YUAN, Wei, LINNARTZ, Jean-Paul MG, et NIEMEGEERS, Ignas GMM. Adaptive CCA for IEEE 802.15. 4 wireless sensor networks to mitigate interference. In : 2010 IEEE Wireless Communication and Networking Conference. IEEE, 2010. p. 1-5.
[65] ORFANIDIS, Charalampos, FEENEY, Laura Marie, JACOBSSON, Martin, et al. Cross-technology Clear Channel Assessment for Low-Power Wide Area Networks. In : The 16th IEEE International Conference on Mobile Ad-Hoc and Smart Systems. 2019.
[66] BEZUNARTEA, Maite, BANH, Mai, GAMALLO, Miguel, et al. Impact of cross-layer interactions between radio duty cycling and routing on the efficiency of a wireless sensor network: A testbed study involving contikiMAC and RPL. In : Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing. 2017. p. 1-7.
[67] ns-3 Network Simulator (online) https://www.nsnam.org/
[68] https://standards.ieee.org/standard/802_11-2016.html#Standard
[69] JIANG, Li Bin et LIEW, Soung Chang. Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks. IEEE Transactions on Mobile Computing, 2007, vol. 7, no 1, p. 34-49.
[70] KOLAHI, Samad S. Comparison of FDMA. TDMA and CDMA system capacities. In : Proceedings of the 10th WSEAS international conference on Communications. World Scientific and Engineering Academy and Society (WSEAS), 2006. p. 333-336.
[71] DEMIRKOL, Ilker, ERSOY, Cem, et ALAGOZ, Fatih. MAC protocols for wireless sensor networks: a survey. IEEE Communications Magazine, 2006, vol. 44, no 4, p. 115-121.
[72] SOHRABI, Katayoun et POTTIE, Gregory J. Performance of a novel self-organization protocol for wireless ad-hoc sensor networks. In : Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324). IEEE, 1999. p. 1222-1226.
[73] https://standards.ieee.org/standard/802_3an-2006.html
[74] YE, Wei, HEIDEMANN, John, et ESTRIN, Deborah. An energy-efficient MAC protocol for wireless sensor networks. In : Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, 2002. p. 1567-1576.
[75] VAN DAM, Tijs et LANGENDOEN, Koen. An adaptive energy-efficient MAC protocol for wireless sensor networks. In : Proceedings of the 1st international conference on Embedded networked sensor systems. 2003. p. 171-180.
[76] POLASTRE, Joseph, HILL, Jason, et CULLER, David. Versatile low power media access for wireless sensor networks. In : Proceedings of the 2nd international conference on Embedded networked sensor systems. 2004. p. 95-107.
[77] EL-HOIYDI, Amre et DECOTIGNIE, Jean-Dominique. WiseMAC: An ultra low power MAC protocol for multi-hop wireless sensor networks. In : International symposium on algorithms and experiments for sensor systems, wireless networks and distributed robotics. Springer, Berlin, Heidelberg, 2004. p. 18-31.

[78] BUETTNER, Michael, YEE, Gary V., ANDERSON, Eric, et al. X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In : Proceedings of the 4th international conference on Embedded networked sensor systems. 2006. p. 307-320.
[79] BARONTI, Paolo, PILLAI, Prashant, CHOOK, Vince WC, et al. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. Computer communications, 2007, vol. 30, no 7, p. 1655-1695.
[80] https://www.linuxembedded.fr/2020/03/introduction-au-sigfox/
[81] Sigfox technical overview
[82] https://www.wndgroup.io/2020/01/13/iot-arms-race-is-on-sigfox-promises-1bn-connections-in-three-years/
[83] https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf
[84] https://qrcline.com/lora-wan/packet-format
[85] https://www.rfwireless-world.com/Tutorials/NB-IoT-tutorial.html
[86] MEKKI, Kais, BAJIC, Eddy, CHAXEL, Frederic, et al. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 2019, vol. 5, no 1, p. 1-7.
[87] BOUAZZI, Imen, BHAR, Jamila, et ATRI, Mohamed. Priority-based queuing and transmission rate management using a fuzzy logic controller in WSNs. ICT Express, 2017, vol. 3, no 2, p. 101-105.
[88] CHU, Yi, MITCHELL, Paul D., et GRACE, David. ALOHA and Q-learning based medium access control for wireless sensor networks. In : 2012 International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2012. p. 511-515.
[89] COLLOTTA, Mario, CASCIO, Arcangelo Lo, PAU, Giovanni, et al. A fuzzy controller to improve CSMA/CA performance in IEEE 802.15. 4 industrial wireless sensor networks. In : 2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA). IEEE, 2013. p. 1-4.
[90] EL CHALL, Rida, LAHOUD, Samer, et EL HELOU, Melhem. LoRaWAN network: radio propagation models and performance evaluation in various environments in Lebanon. *IEEE Internet of Things Journal*, 2019, vol. 6, no 2, p. 2366-2378.
[91] http://deeplearning.net/tutorial/contents.html#
[92] POPESCU, Marius-Constantin, BALAS, Valentina E., PERESCU-POPESCU, Liliana, *et al.* Multilayer perceptron and neural networks. *WSEAS Transactions on Circuits and Systems*, 2009, vol. 8, no 7, p. 579-588.
[93] SCHMIDHUBER, Jürgen. Deep learning in neural networks: An overview. *Neural networks*, 2015, vol. 61, p. 85-117.
[94] YAMASHITA, Rikiya, NISHIO, Mizuho, DO, Richard Kinh Gian, *et al.* Convolutional neural networks: an overview and application in radiology. *Insights into imaging*, 2018, vol. 9, no 4, p. 611-629.
[95] O'SHEA, Keiron et NASH, Ryan. An introduction to convolutional neural networks. *arXiv preprint arXiv:1511.08458*, 2015.
[96] ADEGE, Abebe Belay, LIN, Hsin-Piao, et WANG, Li-Chun. Mobility Predictions for IoT Devices Using Gated Recurrent Unit Network. *IEEE Internet of Things Journal*, 2019.